Intel® Education

Theft Deterrent server

User Manual

December 2014

Legal Notices

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The API and software may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright © 2011 Intel Corporation.

* Third party names and brands may be claimed as the property of others.

Table of Contents

1. Introduction 1
1.1 Document purpose and scope 1
1.2 Terminology 1
1.2.1 Abbreviations 1
1.3 Revision History 1
2. Overview 2
2.1 Browser Requirements 2
2.2 How Theft Deterrent server Works 2
2.2.1 Main Scenarios 3
2.3 Server Support Mode 4
2.4 User Accounts 4
3. User Login 6
4. Home 7
5. Inventory 8
5.1 Approve New Device 8
5.2 View Device Details 9
5.3 Assign Group 9
5.4 Lock and Unlock Devices 10
5.4.1 Lock Devices 10
5.4.2 Allow unlocking 10
5.4.3 Generate Unlock Code 11
5.5 Provision New Certificate 11
5.6 Reject and Delete Device 12
5.7 Online Transfer Device 13
5.7.1 Steps to Transfer Device Out 13
5.7.2 Steps to Transfer Device In 14
5.7.3 Steps to Transfer Locked Device 14
6. Groups & Accounts 15
6.1 Manage Groups 15
6.2 Manage Accounts 15
7. Settings 17
7.1 General Settings 17
7.1.1 Offline Boot Certificate 17
7.1.2 Import Device(s) 18
7.1.3 Email Notification 19
7.1.4 SMS Notification 19
7.2 Server Settings 20
7.2.1 Set Up Automatic Server Broadcast 21
7.2.2 Set Up Automatic Device Approval 21
7.2.3 Set Up E-mail Server 22
7.2.4 Support E-mail 22
7.3 Client Settings 23
7.3.1 Configure Global Certificate 23
7.3.2 Configure Check-in Interval 23
7.3.3 Set Client Password Protection 24
7.3.4 Configure Student Unlock Code 24
7.3.5 Unknown Device Remote Unlock 24
7.4 Security Settings 25
7.4.1 Update Public Key 25
7.4.2 Update Shared Secret 26
7.4.3 Export the Public Key 27
7.4.4 Import Pre-activated Package 28

7.4.5 Recover Crashed Server 28
7.4.6 Offline Transfer 28
7.5 Advanced Settings 34
7.5.1 Set Up Server Name and Address 34
7.5.2 Activate Theft Deterrent Server (Stand-alone mode & your own Root Public Key) 34
7.5.3 Reregister or Reactivate Theft Deterrent Server 35
7.5.4 Back Up Theft Deterrent Server 36
7.5.5 Restore Theft Deterrent Server 38
7.5.6 Set Up Smart Client Upgrade 39
7.6 Account Settings 41
8. Troubleshooting 42
8.1 Warning and Error Messages 42
8.2 Device Error Codes 42
8.3 Client Unlock Screen Error Codes 43
8.4 Smart Client Upgrade Error Codes 43
8.5 Register/Activate Error Codes 44
8.6 The Root Public Key file is missing 44
8.7 The server keystore file is corrupted 45
8.8 The server failed to load configuration files 45
8.9 The server failed to connect to the database 45
8.10 Error 404: Page not found 46
8.11 Theft Deterrent server activation problem 46
9. FAQ 47
10. Glossary 50
Appendix A. Device Status 51
Appendix B. Notification Table 52

List of Figures

Figure 1 - Defining and Deploying Security Policy 3
Figure 2 - Lock Stolen Devices 3
Figure 3 - Device Normal Usage 4
Figure 4 - Server Webpage 6
Figure 5 - Inventory Summary and Device Statistics 7
Figure 6 - Notifications 7
Figure 7 - Pending New Devices Example 9
Figure 8 - Assign to Group 10
Figure 9 - Manage Devices (Lock & Unlock) 10
Figure 10 - Change Boot Tick 11
Figure 11 - Provision New Certificate 12
Figure 12 - Transfer Device 13
Figure 13 - Offline Boot Certificate 17
Figure 14 - Set Up E-mail Notification 19
Figure 15 - TD SMS application in Android Phone 20
Figure 16 - Set Up SMS Notification 20
Figure 17 - Automatic Server Broadcast 21
Figure 18 - Automatic Device Approval 21
Figure 19 - Set Up E-mail Server 22
Figure 20 - Set Up E-mail Server 22
Figure 21 - Global Certificate 23
Figure 22 - Check-in Interval 23
Figure 23 - Student Unlock Code 24
Figure 24 - Unknown Device Remote Unlock 24
Figure 25 - Update Public Key 25
Figure 26 - Update Public Key Offline 26
Figure 27 - Update Shared Secret 27
Figure 28 - Export the Public Key 27
Figure 29 – Import Transfer-in Package 29
Figure 30 – Import Transfer-in Package 29
Figure 31 – View Transfer-in Package 29
Figure 32 – Import Transfer-out Package 30
Figure 33 – Import Transfer-out package 30
Figure 34 – Input Destination server name and URL 31
Figure 35 – View Transfer-out Package 31
Figure 36 – Transfer Device under two modes 32
Figure 37 – Transfer-out page 32
Figure 38 – Activate Server 35
Figure 39 – Reregister Server 35
Figure 40 – Reactivate Server 36
Figure 41 - Back Up Server with the Stand-alone Mode 37
Figure 42 - Back Up Server with the Central Server Supported Mode 38
Figure 43 - Restore Server 39
Figure 44 - Smart Client Upgrade 40
Figure 45 - Configure Download Server 40
Figure 46 - Account page 41
Figure 47 - Server Error (1) 44
Figure 48 - Server Error (2) 45
Figure 49 - Server Error (3) 45
Figure 50 - Server Error (4) 45

1. Introduction

1.1 Document purpose and scope

This document introduces the background and functions of the Intel® Education Theft Deterrent server version 4.x.

The intended audience of this document includes Theft Deterrent server users and support personnel of the Theft Deterrent system.

1.2 Terminology

1.2.1 Abbreviations

Abbreviation	*Description*
server	Theft Deterrent server
client	Theft Deterrent client

1.3 Revision History

Revision	*Date*	*Comment*
V0.62	2013/9	**Device History** change to **Device Statistics, Pending Approvals** change to **Pending New Devices.** Update Figure 5,7,22,23,28,29 Add **Import Device(s)** and move the **Offline Boot Certificate**
V0.63	2013/11	Add **Export Report**, **Lock** awaiting for check-in device, **SMS Notification**, **Notification table,** central server register/activate error code
V0.64	2014/1	Update Figure 5, 23, Device detail and add one error code and error action, add **Download Log**.
V0.65	2014/3	Add Export Logs, Update **Generate Unlock Code**, Add **Reject Device,** Update transfer out server address, Update **Import device(s)**, Add **Export the Public Key** and Update copy download package description.
V0.66	2014/6	Update Section 7.4.4 Import Pre-activated package and Section 7.4.5 Recover Crashed Server. Add Section 7.4.6 Offline Transfer. Update Section 7.5.3 Reregister or Reactivate TD server. Add Section 8.3 Client Unlock Screen Error Codes. Add Figure37. Add Section 7.2.4 Support E-mail. Update Figure 14.

2. Overview

The Theft Deterrent server (server) is the server component of Theft Deterrent system, which is designed to deter theft of Intel® Education Tablet and Intel® classmate PC. The server allows device owner such as school administrator to lock the device if it is lost or stolen.

Note: The term device is used throughout the document to refer to Intel® Education Tablet and Intel® classmate PC.

2.1 Browser Requirements

The server is web based and accessed by web browsers. The supported web browsers are as follows:

- Firefox
- Chrome
- Internet Explorer 8 or above

To access the server with Internet Explorer, add the server URL to **Trusted sites** with the following steps:

1. On Internet Explorer, click **Tools** -> **Internet Options** -> **Security Tab**.
2. On the **Security** page, select **Trusted Sites** and click the **Sites** button.
3. On the popup window, input https://*[serverURL]*/ and then click the **Add** button.

Click **Yes** on the confirmation window. Click **Close**.
Make sure that the security level for **Trusted sites** is **Medium** and then click **OK**.

2.2 How Theft Deterrent server Works

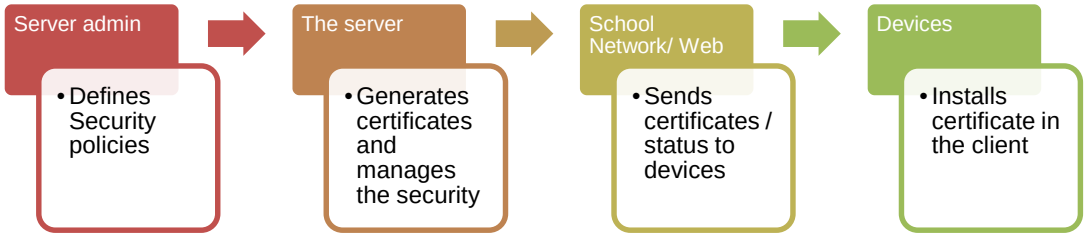
The server manages devices based on a set of security policy, which consists of two configurable settings:

- **Expiration Date**: Number of days in which the device can be used.
- **Remaining Cycles**: Number of times that the device can change its energy state. For example, suspension mode, hibernation, reboot, etc. This is not applicable to Intel® Education Tablet.

Once the policy is defined, it is deployed to devices in the form of digital certificate. During normal usage, you can provision the following certificates to devices to update their security policy:

- **Global Certificate**: A device downloads and applies this certificate from the server automatically when its current certificate is about to expire.
- **Temporary Certificate**: You can provision this certificate to devices that would not be able to connect with the server for a certain period of time. For example, the device owner goes on vacation for 1 month.
- **Permanent Certificate**: You can provision this certificate to devices that are not required to connect with the server anymore. For example, the device owner graduates.

Figure 1 - Defining and Deploying Security Policy



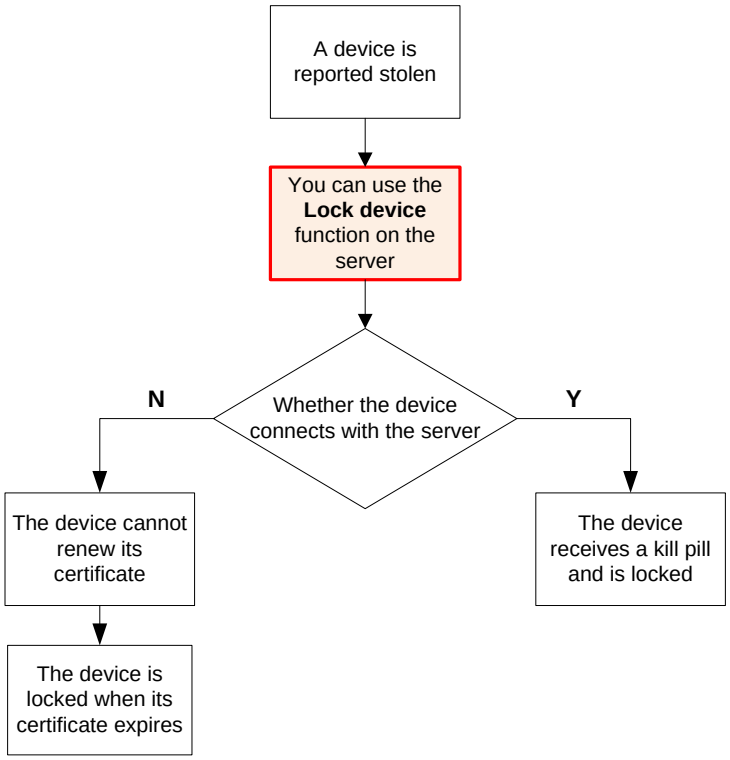
If security policy violation is detected, the device is locked. Also, you can manually lock devices from the server, and a kill pill will be sent to the device once it connects with the server.

2.2.1 Main Scenarios

The security policy and digital certificates introduced above enables the server to lockdown devices when needed. The main scenarios are as follows:

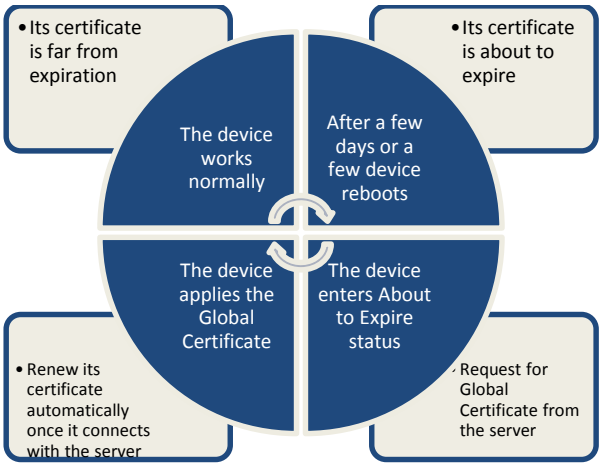
The server can lock devices, for example, when the device is lost or stolen. The typical scenario is as follows:

Figure 2 - Lock Stolen Devices



During normal usage, a device can renew its certificate automatically by connecting to server regularly. No further action is required on the server side.

Figure 3 - Device Normal Usage



2.3 Server Support Mode

The server is installed with one of the following mode:

Server Support Mode	*Description*
Stand-alone mode with the Intel Root Public Key	• No activation is required after the installation.
Stand-alone mode with your own Root Public Key	• You can use the server without activation. • You can activate the server. (The server transforms to the **Central Server supported** mode)
Central Server supported mode	• You must activate the server during pre-configuration after installation completes.

The functionalities that you access differ according to the server support mode. If your server runs with the **Central Server supported** mode, you can access the extended functionalities of the server to achieve the following tasks:

- Register the school information of the server on the central server.
- Save a copy of the server key files on the central server.
- Manage the devices pre-activated in factory.
- Transfer devices via the central server to other servers.

2.4 User Accounts

The master admin account is created by default during the server installation. You can create program admin, helpdesk, and custom accounts from the **Groups & Accounts** page. The accounts are assigned with different access rights:

Server Webpages	*Master Admin*	*Program Admin*	*Helpdesk / Call Center*	*Custom*
Home	√	√	√	√
Inventory	√	√	√	√
Groups & Accounts	√	√		

Settings	General	√	√	√	√
	Client	√	√		
	Server	√	√		
	Security	√	√		
	Advanced	√			
	Account			√	√

Each user can only access the functionalities and devices assigned to his/her user account.

Account	*Account Type*	*Functions*	*Groups*
Master Admin	Admin	All functions.	All groups.
Program Admin	Admin	All functions except the **Advanced** page under **Settings**.	All groups.
Helpdesk / Call Center	Non-admin	**Lock Device** and **Generate Unlock Code/Package**.	The groups assigned.
Custom	Non-admin	The functions assigned.	The groups assigned.

3. User Login

Open the webpage of the server with the following URL, where ***[serverURL]*** is the IP address or hostname of the server.

- https://*[serverURL]*/TheftDeterrent

Log in the server with your username and password. To log in with the master admin account, use the following credentials:

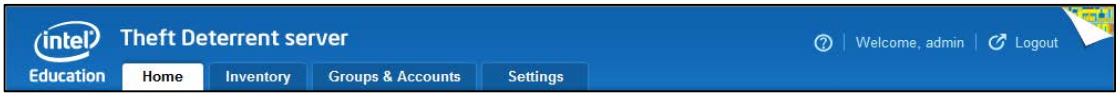
- The username is **admin**
- The password is the one set during the installation process.

If you forgot your password, click the **Forgot password?** link to reset your password. However, your user account must contain an e-mail address and the e-mail server must be set up before you can reset your password, otherwise, you have to contact the server administrator for help.

The **Home** page is displayed after you log in the server. You can click the tabs next to the **Home** page to access other functionalities. However, if you are logging in for the first time, you might need to complete your account information before accessing the **Home** page.

Note: The master admin must complete the pre-configuration before any user can access the **Home** page. For more information about server pre-configuration, see the Intel® Education Theft Deterrent Deployment Guide.

Figure 4 - Server Webpage



4. Home

The **Home** page displays a statistical report about the devices that you manage. The report contains three sections: **Inventory Summary**, **Device Statistic**, and **Notifications**. You can click the links in the reports to view detailed information.

Figure 5 - Inventory Summary and Device Statistics

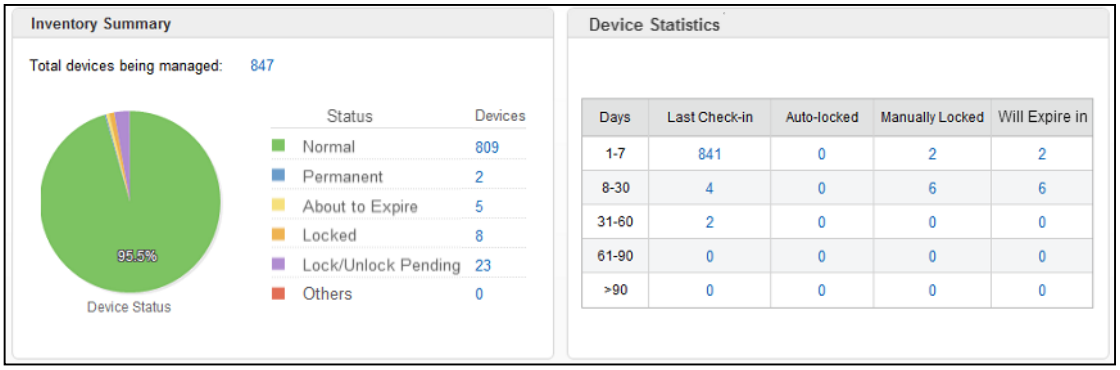
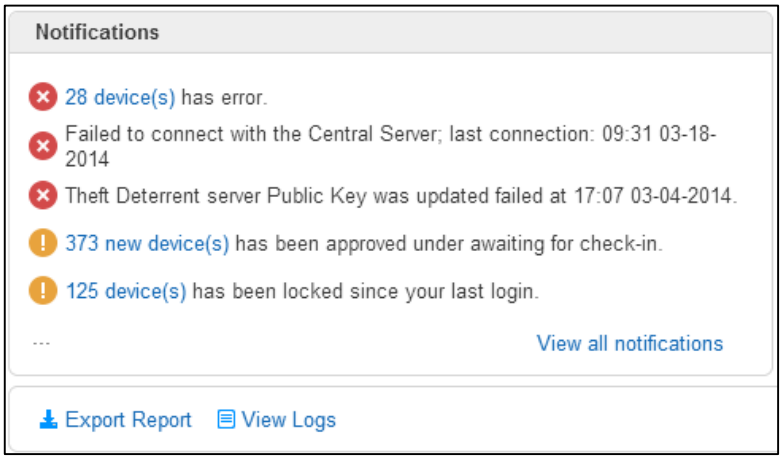


Figure 6 - Notifications



Inventory Summary

For information about the device status, see Appendix.

Notifications

You can view notifications when certain events occur. There are three types of notifications:

- **Error**: Might require your action.
- **Reminder**: Might require your action.
- **Information:** No action is required.

For detail content of the notification, see Appendix.

Click the **Export Report** can export some or all information of the dashboard to a .CSV file.

Click the **View Logs** to view, filter or export the server operation logs.

5. Inventory

On the **Inventory** pages, you can manage the devices. The pages include the following functions:

- Approve new devices
- Assign devices to groups
- View device details
- Lock and unlock devices
- Provision new certificate
- Reject and delete device(s)
- Transfer devices

Note: You can only access the functions assigned to your user account.

5.1 Approve New Device

Before you can manage a device, the server must approve the device to enable the Theft Deterrent function on the client. This process is named client activation.

By default, the server is set to approve devices automatically and no action is required. If you want to approve devices manually, turn off the Automatic Device Approval function on the **Server** page under **Settings**.

Requirements: Ensure that the client is in **Inactive** status and is connected with the server.

Steps:

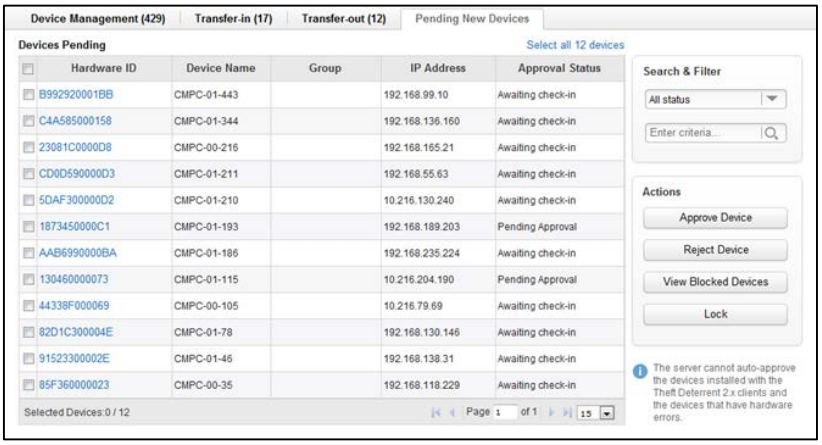
To approve new devices, follow these steps:

1. When there are devices pending for approval, a **Pending New Devices** tab appears under **Inventory**. Click the tab to open the **Pending New Devices** page.

Select the device that you want to approve.
Click the **Approve Device** button and then click **OK** on the confirmation window. The status of the device is changed to **Awaiting check-in**.
After the device downloads and parses the certificate, the device record is moved to the **Device Management** page and the status of the device is changed to **Normal**.

If you reject a device, the device record will be moved to the blocked devices list and you can view the list by clicking the **View Blocked Devices** button. To approve a rejected device, you must first remove the device record from the blocked devices list.

Figure 7 - Pending New Devices Example



Note: You can lock device(s) in Awaiting for check-in status. The record(s) will be moved to the Device Management page with Lock Pending and the device(s) will be restarted and then locked after receiving the lock command.

5.2 View Device Details

You can open the **Device Details** page by clicking the **Hardware ID** of a device on the **Device Management** page.

For devices in **Normal**, **Permanent**, or **About to Expire** status, you can edit the following information by clicking the **Edit Device** button on the **Device Details** page:

- Assigned group
- Student name and email
- Student password of the server webpage for students
- Comment

5.3 Assign Group

If you are managing a large number of devices, you can assign the devices to different groups to manage them more efficiently.

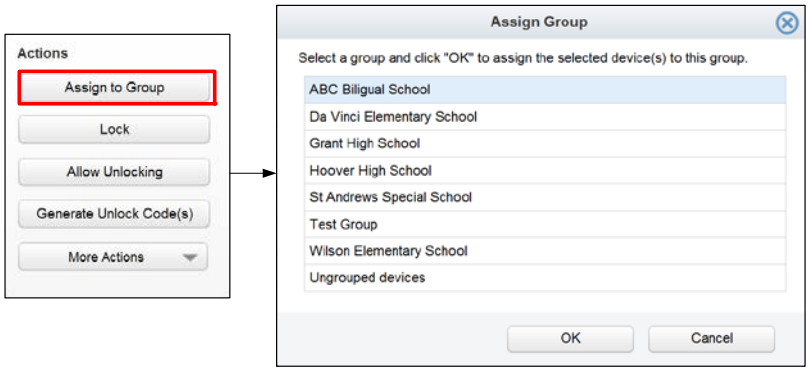
Requirements: The master admin or a program admin must first create the groups on the **Groups & Accounts** page.

Steps:

To assign a device to a group, follow these steps:

1. On the **Device Management** page, select the device that you want to assign to a **Group**. Click the **Assign to group** button in the **Actions** area.
Select a group and then click **OK**.

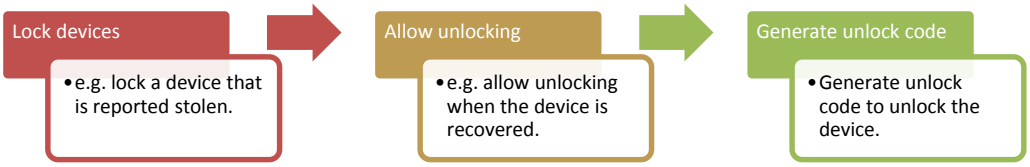
Figure 8 - Assign to Group



5.4 Lock and Unlock Devices

You can manually lock or unlock devices as follows.

Figure 9 - Manage Devices (Lock & Unlock)



5.4.1 Lock Devices

To lock a device, follow these steps:

1. On the **Device Management** page, select the device that you want to lock.
Click the **Lock** button in the **Actions** area.
On the **Lock Device** window, input a lock comment and then click **Lock Device**.
Click **Yes** on the confirmation window. The status of the device is changed to **Lock Pending**.

Once the device connects with the server, it downloads a kill pill and is locked after a mandatory reboot. The status of the device is then changed to **Manually Locked** on the server webpage.

Note: When a device is locked, the user will not be able to access the operating system.

5.4.2 Allow unlocking

To unlock a device that is in **Manually Locked** or **Lock Pending** status, you must first allow the device for unlocking. Follow these steps:

1. On the **Device Management** page, select the device in **Manually Locked** or **Lock Pending** status that you want to unlock.
Click the **Allow Unlocking** button in the **Actions** area.
Click **Yes** on the confirmation window.

When the action completes, the status of the device is changed:

- If the device had been in **Manually Locked** status, the status is changed to **Unlock Pending**. You can now generate an unlock code for the device and then unlock it by inputting the unlock code on its lock screen.
- If the device had been in **Lock Pending** status, the status returns to the previous one (**Normal**, **About to Expire**, or **Permanent**) and no further action is required.

5.4.3 Generate Unlock Code

You can unlock a device by generating an unlock code from the server and then inputting the unlock code on the lock screen of the device.

To generate an unlock code for a device, follow these steps:

1. On the **Device Management** or **Pending New Device(s)** page, select the device that you want to unlock.

Click the **Generate Unlock Code** button in the **Actions** area.
Check the **Boot Tick** number displayed in the table.
If the **Boot Tick** is different from that displayed on the lock screen of the device, click the **Boot Tick** number in the table to change the value according to the number on the lock screen.

Figure 10 - Change Boot Tick

Hardware ID	Device Name	Boot Tick	Unlock Code
B0825348887B	android_92dc8390dc82016a	6	4016007013
49DCDD0001ED	CMPC-01-493	18	5122761142

Record the unlock code displayed.

You can now unlock the device by inputting the unlock code on its lock screen.

Note: The client might not be able to download certificates any more if the **Boot Tick** number you entered on the **Generate Unlock Code** window differs largely from the **Boot Tick** in the device. Therefore, make sure that the following requirement is met:

Device **Boot Tick** -5 <= The **Boot Tick** you input on the server <= Device **Boot Tick** +1

If you cannot generate unlock code for a device and see a warning icon in the **Unlock Code** column, check the tool tip of the icon and follow one of these solutions:

Tool tip	*Solution*
Manually locked	Allow unlocking for the device before generating the unlock code.
Shared Secret does not exist.	Update the Shared Secret for the device before generating the unlock code.
Shared Secret error.	Update the Shared Secret for the device before generating the unlock code.

Note: If a device has been locked and cannot sync-up the Shared Secret with server, you can Export the Shared Secret and offline apply it to the locked device in advance.

5.5 Provision New Certificate

You can provision one of the following certificates to a device to update its security policy:

- **Provision a temporary certificate**: Set the values of the Expiration Date and the Remaining Cycles for the device.

- **Provision a permanent certificate:** Set the certificate to a permanent value so that the device will never be automatically locked.

Note: The **Remaining Cycles** is not applicable to Intel® Education Tablet.

Requirements: You can only provision new certificates for devices in **Normal**, **About to Expire**, and **Permanent** status.

Steps:

To provision a new certificate for a device, follow these steps:

1. On the **Device Management** page, select the device that you want to provision a new certificate to.

Click the **Provision New Certificate** button in the **Actions** area. The button might be located in **More Actions**.
On the **Provision New Certificate** window, select one of the following options.

- **Provision a temporary certificate**
- **Provision a permanent certificate**

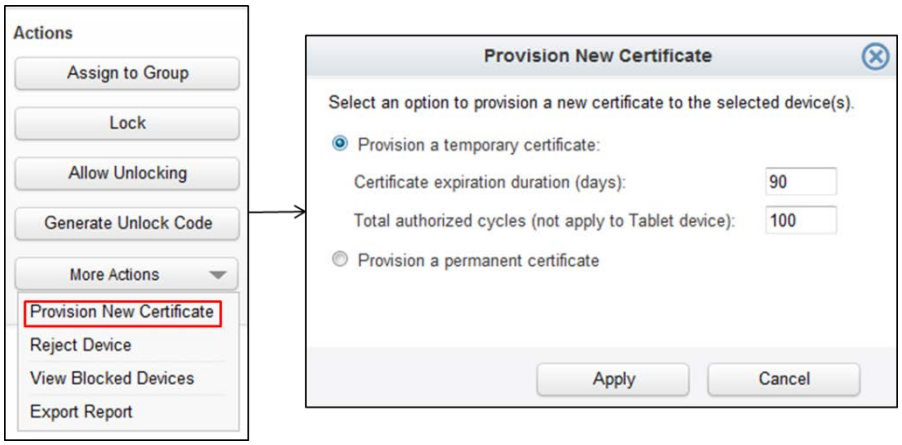
If you select the **Provision a temporary certificate** option, input the following values for the new certificate.

- **Certificate expiration duration:** the number of days before the certificate expires.
- **Total authorized cycles**: the number of **Remaining cycles**.

  Note: The **Total authorized cycles** is not applicable to Intel® Education Tablet.

Click **Apply**.

Figure 11 - Provision New Certificate



The **Expiration date** and the **Remaining cycles** displayed on the **Device Management** page are changed after the device downloads and parses the new certificate.

5.6 Reject and Delete Device

To reject, restore or delete device(s), follow these steps:

1. On the **Device Management** or **Pending New Devices** page, select the device(s) you want to reject.
2. Click the **Reject Device** button in the **Actions** panel.

3. Click **Yes** on the confirmation window, then the device(s) will be moved to the blocked list. The server cannot manage the device in the blocked list. Once the client connects with the server, the client will display the Device is Rejected.
4. To restore the device to its previous status, you can click the **View Blocked Devices** button in the **Actions** panel and click **Restore** button to recover it.
5. For server administrators, you can delete the devices permanently by clicking **Remove** button in the **View Blocked Devices** page.

5.7 Online Transfer Device

When a student transfers from your school to a school managed by another server, you can transfer the student's device from your server to that server.

There are two ways to transfer devices.

- Online Transfer: valid only for the server with Central Server Supported Mode
- Offline Transfer: valid for server with any mode.

This section introduces the method the operation steps for **Online Transfer**. As to Offline Transfer, please refer to Offline Transfer-out.

Note: During the transfer process, the servers communicate through the central server to exchange data. The frequency of the communication is defined by the central server heartbeat interval, which defaults to 20 minutes.

Requirements: The servers must be activated on the same central server.

Steps:

The transfer process is as follows:

1. On the original server, request to transfer the device to another server.
2. On the destination server, accept the device to be transferred in.

During the transfer process, a **Transfer-out** tab is displayed on the original server and a **Transfer-in** tab is displayed on the destination server. These tabs appear only when the server has devices pending to be transferred out or in.

Figure 12 - Transfer Device

If a device is locked during the transfer process, you can transfer the locked device.

5.7.1 Steps to Transfer Device Out

To transfer a device to another server, follow these steps:

1. On the **Device Management** page, select the device that you want to transfer.
2. Click the **Transfer** button in the **Actions** area. The button might be located in **More Actions**.
3. On the **Transfer Device** window, select the destination server name from the drop-down list and input the server address. Then click **Transfer Device**.

Note: The server address is IP address or URL of the destination server. The client will automatically update the server address after applying the transfer school package and restart.

The device record is moved to the **Transfer-out** page under **Inventory**. Make sure that you connect the device to the destination server after it is accepted by the destination server.

When transfer completes, the device record is removed from the **Transfer-out** page and added to transfer history.

Note: You can only request to transfer devices in **Normal**, **About to Expire**, or **Permanent** status.

5.7.2 Steps to Transfer Device In

When a device is requesting to be transferred to your server, follow these steps to accept the device:

1. On the **Transfer-in** page under **Inventory**, select the device in **Pending Acceptance** status.
2. Click the **Accept Transfer** button in the **Actions** area. The status of the device is changed to **Awaiting check-in**.
3. Connect the device to your server to download and parse the transfer package. The device reboots automatically when completed.
4. Connect the device to your server again to complete the transfer process.

When transfer completes, the device records are moved to the **Device Management** page.

Note: You can only accept or reject devices in **Pending Acceptance** status. The devices in **Awaiting check-in** status can download the transfer package from either the original or the destination server.

If you failed to accept or reject a device, follow one of these solutions:

- If the status of the device is still **Pending Acceptance**, make sure that the server is connected with the central server and then accept or reject the device again.
- If the status of the device is changed to **Error**, reject the device and then re-start the transfer process from the beginning.

5.7.3 Steps to Transfer Locked Device

If a device is locked during the transfer process and therefore cannot download the transfer package online, you can export the transfer package from either the original or the destination server to transfer the locked device.

To transfer a locked device, follow these steps:

1. On the **Transfer-in** page or the **Transfer-out** page under **Inventory**, select the device that is locked.
2. Click the **Export School Package** button in the **Actions** area and select a location to save the package.
3. Copy the package to a removable disk and then import the package to the locked device. The device is unlocked after the package is imported successfully.
4. Connect the device to the destination server to complete the transfer process.

Note: You cannot export school packages for devices in **Pending acceptance** status. Make sure that you select only one device each time.

If a device is locked after it downloads the transfer package but before the transfer process is completed on the servers, unlock the device with an Offline Boot Certificate.

6. Groups & Accounts

You can create groups and accounts to manage the access rights of server users by assigning users with different user roles and groups.

After server deployment, only the master admin can log in the server who can then create accounts for new users. It is recommended that you provide new users with different access permissions according to their responsibilities.

Note: You must log in as the master admin or a program admin to access this page.

6.1 Manage Groups

When you manage a large number of devices across multiple schools, you can create groups on the server to represent the schools and then assign the devices to different groups to manage the devices more efficiently.

- **Create groups**: click the **Create Group** button, input the group information and then click **Save**.
- **Edit groups**: click the group name in the table.
- **Delete groups**: click the X link in the table.
- **Export groups**: click the **Export** button and save the file to local disk. You can open the file with a text editor such as excel or notepad.
- **Import groups**: you can record the group information in a .CSV file and then import the groups to the server. Follow these steps:

  1) Open an editor to create a file containing the following columns:

Group	*E-mail*	*Phone No.*	*Description*	*Contact Person*

  2) Input the group information in the columns as follows. Make sure the format of the e-mail address is correct.
  3) Save the file and then change the filename extension to **csv**. For example, groups.csv
  4) On the **Groups** page, click the **Import** button to import the groups to the server.

  Note: If your import file contains several groups with the same group name, only the last group with the same group name is imported.

6.2 Manage Accounts

To grant a new user the access permission to the server, you can create an account and assign certain functions and groups to the user.

Steps:

To create an account, follow these steps:

1. On the **Groups & Accounts** page, click the **Accounts** tab and then click the **Create User Account** button.
2. On the **Create User Account** page, input a username.
3. Select a user role. If you select **Custom**, choose the functions that you want to assign to the user. For information about the access rights of different user roles, see User Accounts.
4. Input a password for the account.
5. Input the user's e-mail address and select the following checkbox. The username and password will be sent to this e-mail address when you save the account.
6. Select groups. The user can only access the devices assigned to the selected groups.
7. Input a phone number.
8. Click **Save**.

Note: The password must be 8 to 30 characters in length and must contain at least one lowercase letter [a-z], uppercase letter [A-Z], number [0-9], and special character. It must not contain sequences of the same character (e.g. aa, 33, ##) or numbers that are longer than 5 characters (e.g. 12345, 67890).

For custom accounts with transfer or approve new device permission, make sure that you select **Ungrouped** in **Assign groups** because new devices pending for approval or transfer-in are in **Ungrouped**.

7. Settings

On the **Settings** page, users with the access permissions can configure the general, server, client and security settings. Also, the master admin can access the advanced functions such as the following:

- Activate the server
- Back up the server
- Restore the server
- Smart client upgrade

For information about the access permissions of different user accounts, see User Accounts.

7.1 General Settings

On the **General** page, you can configure the following settings.

- Offline Boot Certificate
- Import Device(s)
- Email Notification
- SMS Notification

7.1.1 Offline Boot Certificate

If a pre-activated device is locked before it is approved and managed by the server, the device is not recorded on the **Device Management** page and therefore you cannot generate an unlock code to unlock the device.

In such cases, if the device was pre-activated with a Public Key in the server keystore, you can export an offline boot certificate to unlock the device.

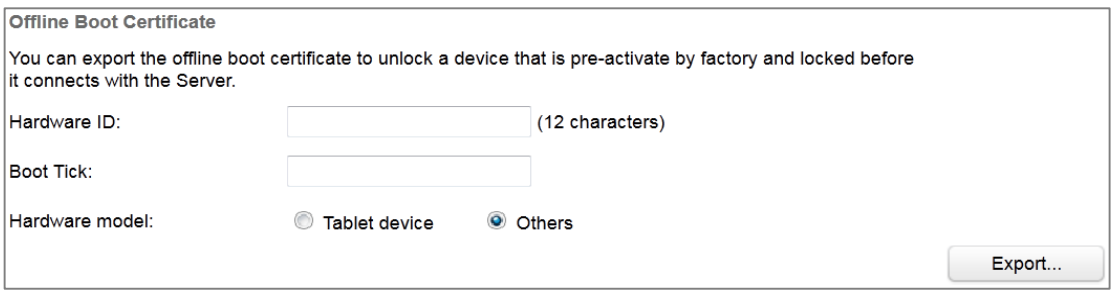
Requirements: You can access the **Offline Boot Certificate** only if you have the right to unlock device.

Steps:

To export the **Offline Boot Certificate**, follow these steps:

1. In the **Offline Boot Certificate** area on the **General** page, input the **Hardware ID** and the **Boot Tick** displayed on the device lock screen.
2. Select the **Hardware model** of your device.
3. Click the **Export** button to export the offline boot certificate named **tcopp.bin** to local disk.

Figure 13 - Offline Boot Certificate



To unlock the device, follow these steps:

1. Copy the offline boot certificate (tcopp.bin) to a removable device.
2. Insert the removable device to the device and import the offline boot certificate.

The device is unlocked after system reboots and you can then manage the device with the server.

7.1.2 Import Device(s)

You can import new device(s) or update device(s) information with a .csv or a zipped .csv file.

Steps:

1. Create a .csv file or modified based on the .csv file exported from Device Management page, which is encoded as UTF-8 and contains one of the following formats. The value(s) of Group column in the .csv file is/are only restricted to the one(s) you are authorized to access.

Hardware ID (Must have)	*Group (Optional)*	*Device Name (Optional)*	*Student Name (optional)*	*Serial No. (Optional)*

Id. de hardware (Must have)	*Grupo (Optional)*	*Nombre de dispositivo (Optional)*	*Nombre de estudiante (optional)*	*N.º de serie (Optional)*

ID do Hardware (Must have)	*Grupo (Optional)*	*Nome do Dispositivo (Optional)*	*Nome do Aluno (optional)*	*Número de Série (Optional)*

Donanım Kimliği (Must have)	*Grup (Optional)*	*Cihaz Adı (Optional)*	*Öğrenci Adı (optional)*	*Seri No. (Optional)*

2. Zip the csv file or split it to several files if the file is larger than 50M.
3. Select **Browse...** for this file and **Import** on the **Server** page under **Import Devie(s)**.

4. Testing for import will start, then a Summary report will be shown:
   a) How many records can be imported as new device(s)
   b) How many records cannot be imported for it has error format
   c) How many records are the same as the existing records in server
   d) How many records are in conflict with the existing records. Do you want to Overwrite or skip?
   e) How many records cannot be imported for invalid group(s)
5. You can Export Report for the testing before Commit the formal import
6. Click **Commit** the import, then the formal import will be started.
7. After import finished, a result will be popup to how many devices are added and how many devices are updated.

7.1.3 Email Notification

You can set up the e-mail notification to receive a summary report of the devices regularly. The report contains the following information:

- The devices that have been automatically or manually locked in the past few days.
- The devices that have not checked in with the server in the past few days.
- The last time when the server was backed up successfully.

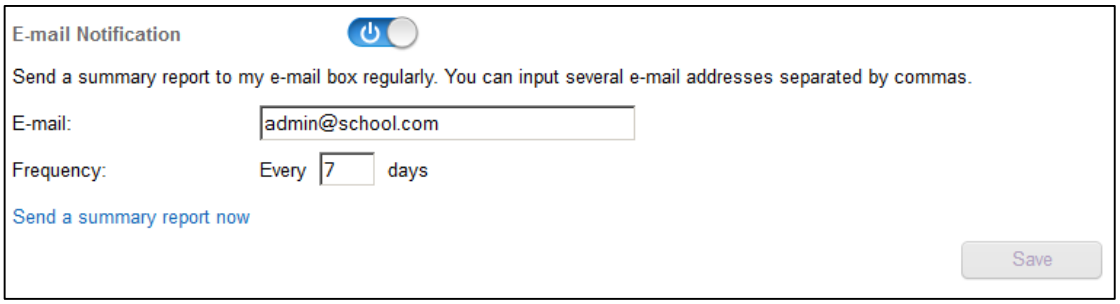
Requirements: The e-mail server must be set up before you can turn on the **E-mail Notification** function.

Steps:

To set up the e-mail notification on the **General** page, follow these steps:

1. Turn on the **E-mail Notification** function.
2. Input one or multiple e-mail addresses to receive the notifications. Separate the e-mail addresses with comma and do not input space between e-mail addresses.
3. Input a number to define the frequency of the notification.
4. Click the **Save** button.

Figure 14 - Set Up E-mail Notification



After you complete the settings, a **Send a summary report now** link appears on the **General** page. You can click the link to send a summary report to the e-mail address immediately. Otherwise, the report is not sent until 12:00 PM after the number of days configured in the frequency box.

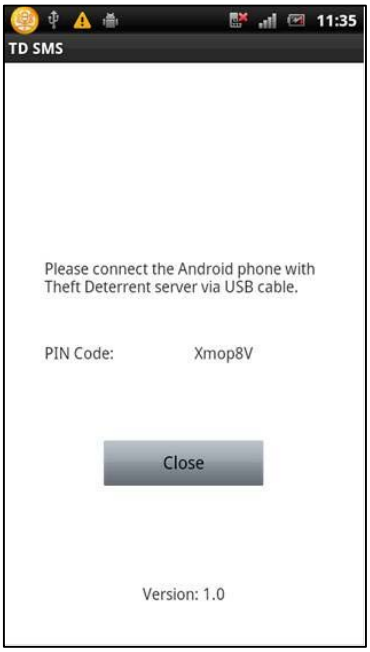
7.1.4 SMS Notification

Besides the email notification, you can also choose to receive similar SMS summary reports with in mobile phones

Requirements:

1. Contact the Support personnel for assistance in configuring the server, installing Android Debug Bridge and Android phone's driver to support the SMS Notification.
2. Install the **TD SMS** application to the Android phone, and then connect the Android phone with server through USB cable.

Figure 15 - TD SMS application in Android Phone

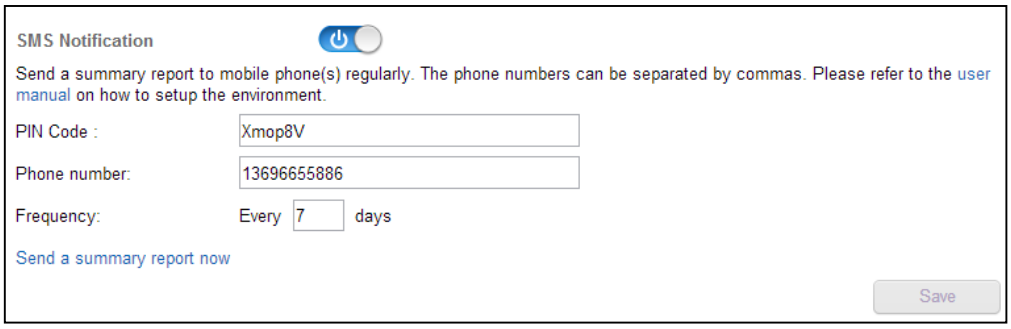


Steps:

To set up the SMS notification on the **General** page, follow these steps:

3. Turn on the SMS Notification function.
4. Input the PIN Code of the connected Android phone used to send summary reports.
5. Input the phone numbers of your receivers. Separate them with commas.
6. Set the frequency of the notification.
5. Click the Save button to finish.

Figure 16 - Set Up SMS Notification



After all the above steps are finished, a **Send a summary report now** link appears. You can click the link to send a summary report to the receivers immediately. Otherwise, the report will be sent until 12:00 PM after the number of days configured in the frequency box.

7.2 Server Settings

On the **Server** page, you can configure the following settings for the server.

- Automatic Server Broadcast
- Automatic Device Approval
- E-mail Server
- Support E-mail

Once the settings are configured correctly, minimal manual changes are needed.

7.2.1 Set Up Automatic Server Broadcast

You can set up the server to broadcast its IP address or URL in LAN so that the devices in the same network will be able to detect and connect to this server automatically.

Requirements:

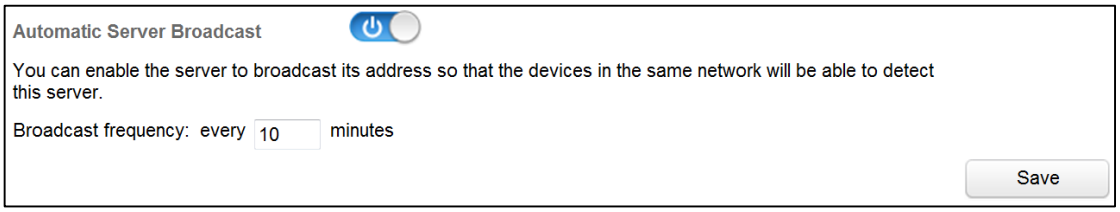
- The master admin must set up the Server Name & Address.
- The server and the clients are deployed in LAN.

Steps:

To set up the **Automatic Server Broadcast** function, follow these steps:

1. Turn on the **Automatic Server Broadcast** function on the **Server** page under **Settings**.
2. Input a number to define the frequency (in minutes).
3. Click the **Save** button.

Figure 17 - Automatic Server Broadcast



7.2.2 Set Up Automatic Device Approval

You can set up the **Automatic Device Approval** function so that the devices in **Inactive** status are activated automatically when they connect with the server.

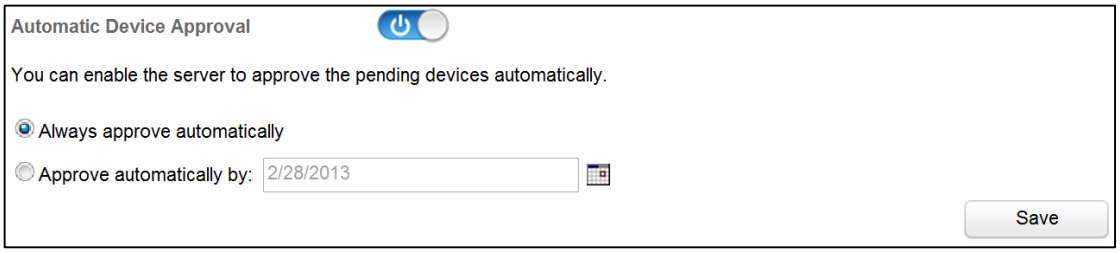
Steps:

To set up the **Automatic Device Approval** function, follow these steps:

1. Turn on the **Automatic Device Approval** function on the **Server** page under **Settings**.
2. Select whether you want to always approve new devices automatically or approve new devices automatically till a certain date.
3. Click the **Save** button.

Note: The server cannot automatically approve the devices that are installed with an earlier version of the client or have hardware errors. In such cases, you must approve or reject the devices manually.

Figure 18 - Automatic Device Approval



7.2.3 Set Up E-mail Server

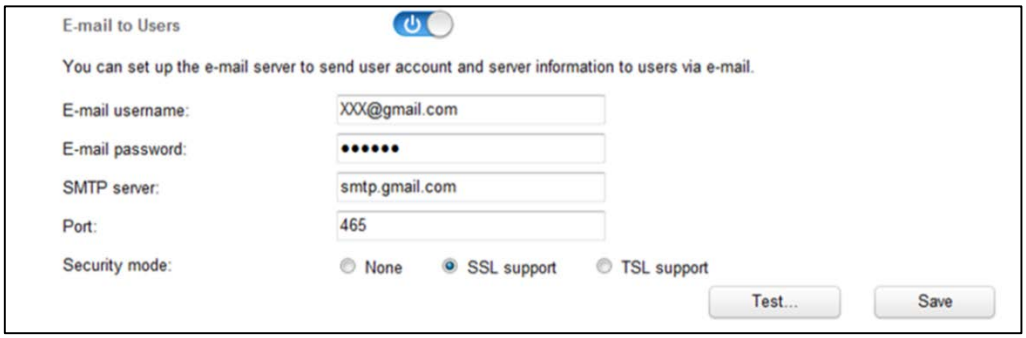
You can set up the e-mail server so that the server can send out e-mails when a user sets up e-mail notifications, forgot his/her password, creates user accounts, etc.

Steps:

To set up the e-mail server, input the following information and then click **Save**.

- **E-mail username**: the e-mail address of your e-mail account
- **E-mail password**: the password of your e-mail account
- **SMTP server**: the hostname of the SMTP server.
- **Port**: the port number of the SMTP server.
- **Security Mode**: select a security mode.

Figure 19 - Set Up E-mail Server



7.2.4 Support E-mail

You can set up the **Support E-mail** function to regularly send your server configuration information as an email to Theft Deterrent support team (tdsupport@intel.com) and your own support e-mail address(es).

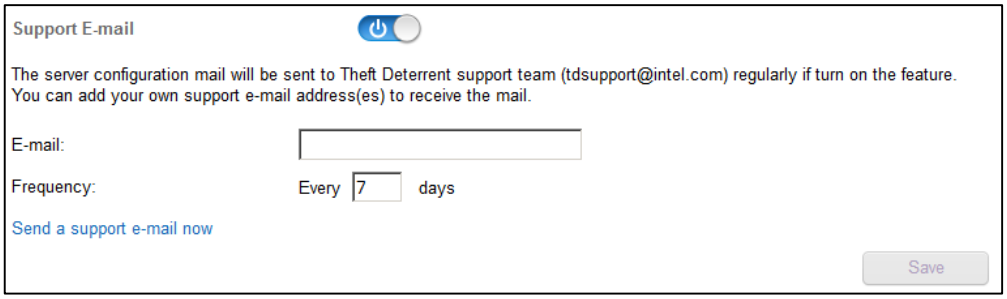
Requirements: The e-mail server must be set up before you can turn on the **Support E-mail** function.

Steps:

To set up the **Support E-mail** function on the **Server** page, follow these steps:

1. Turn on the **Support E-mail** function.
2. If you want to send your server configuration mail to your own e-mail addresses besides Theft Deterrent support team, you can input one or multiple e-mail addresses separated by commas.
3. Input a number to define the frequency of the sending email.
4. Click the **Save** button.

Figure 20 - Set Up E-mail Server



Note: Every time you **Save** settings, you can choose to **Send a summary report now** by clicking the corresponding link.

7.3 Client Settings

On the **Client** page, you can configure the following settings for the client:

- Global certificate
- Check-in Interval
- Password protection
- Student Unlock Code

Once the settings are configured correctly, minimal manual changes are needed.

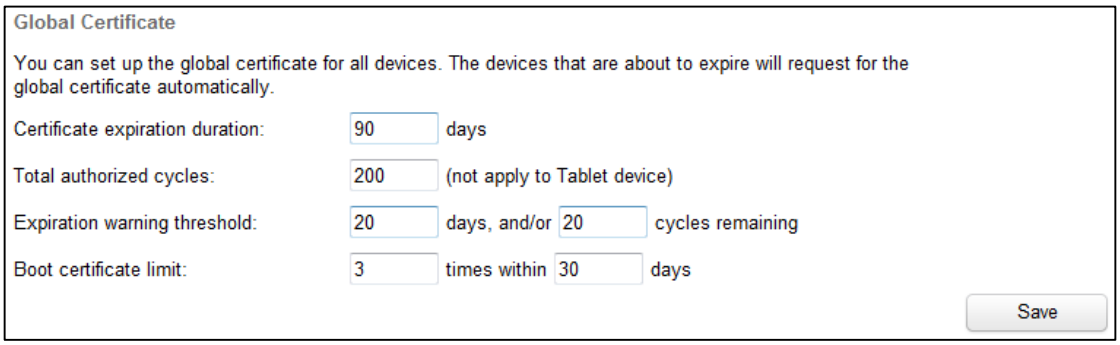
7.3.1 Configure Global Certificate

You can configure the values of the global certificate, which is downloaded automatically by devices in **About to Expire** status to renew their security policy. Also, you can configure the **Expiration warning threshold** to define when a device would enter the **About to Expire** status.

For security reasons, you must also define the maximum number of global certificates that a device can download in a certain time period by configuring the **Boot certificate limit**.

For more information about the security policy, see How Theft Deterrent server Works.

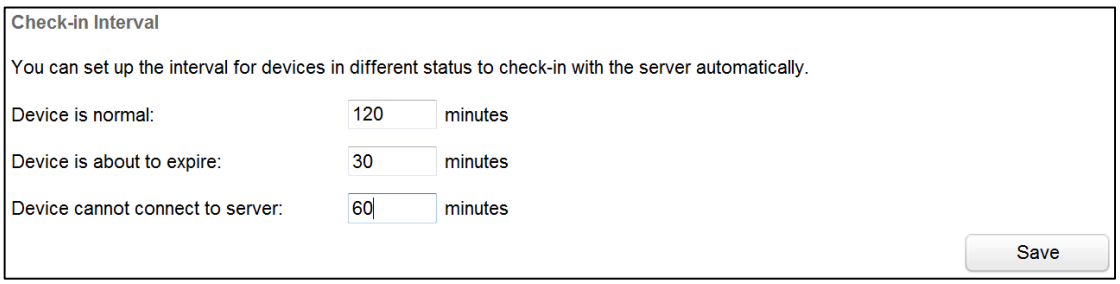
Figure 21 - Global Certificate



7.3.2 Configure Check-in Interval

When a device is connected with the server, it checks in with the server regularly to see if there is a new certificate to download from the server. You can set up the check-in interval (in minutes) for devices in different status.

Figure 22 - Check-in Interval



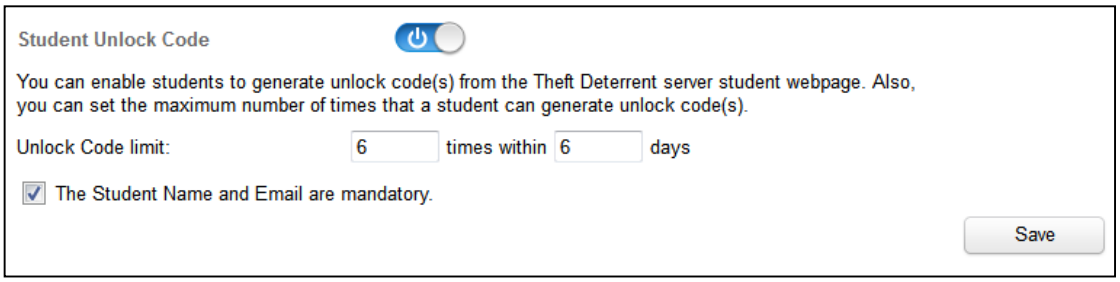
7.3.3 Set Client Password Protection

You can set a password to protect the client. The password is required when a user want to configure or uninstall the client. The password must be less than 30 characters in length.

7.3.4 Configure Student Unlock Code

You can enable students to generate unlock codes from the server webpage for student. Also, you can set the maximum number of times that a student can generate unlock codes within a certain time period.

Figure 23 - Student Unlock Code



Note: The student name and email in webpage could be configured to be mandatory.

7.3.5 Unknown Device Remote Unlock

Intel® Education tablets that are locked automatically can be unlocked remotely through the network and no action is required on the server. However, if a pre-activated device is locked before it is approved and managed by the server, you must turn on **Unknown Device Remote Unlock** to enable the remote unlocking function for the device.

Also, configure the following settings:

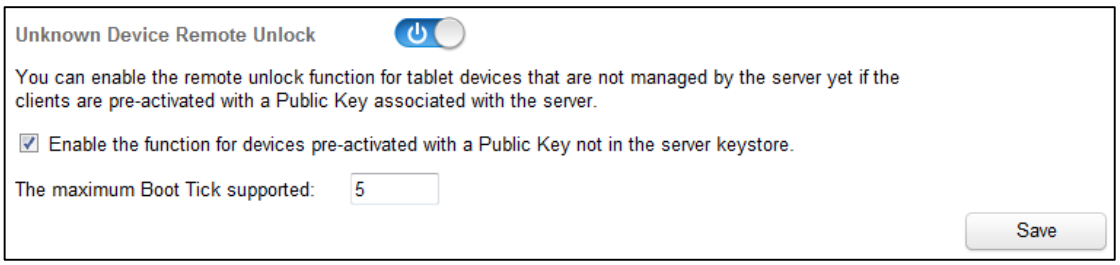
Enable the function for devices pre-activated with a Public Key not in the server keystore.

- By default, the function only unlocks devices pre-activated with a Public Key in server keystore. For devices activated with a different Public Key, you can enable the function by selecting this option and importing the pre-activate or crash recovery package.

The maximum Boot Tick supported:

- For security reasons, you must set a **Boot Tick** number so that only the unknown devices with a Boot Tick smaller than or equals to this number can be unlocked remotely.

Figure 24 - Unknown Device Remote Unlock



7.4 Security Settings

You can access the following functions on the **Security** page under **Settings**.

- Update Public Key
- Update Shared Secret
- Export the Public Key
- Import pre-activated package
- Import crash recovery package
- Offline Transfer

These settings would affect the devices managed by the server. Only use these settings or tools if you are an advanced user.

7.4.1 Update Public Key

If you suspect that the server key pair (public key and private key) is compromised, update the key pair on both the server and the devices with the **Update Public Key** function to keep your server secure.

Steps:

You must first update the key pair on the server and then update the server Public Key on the devices accordingly.

Firstly, update the key pair on the server with the following procedures:

- If your server is not activated on the central server, follow these steps:

    1) On the **Security** page, click the **Update Public Key** button to update the key pair on the server.
    2) On the **Home** page, you will see a notification showing "Theft Deterrent server Public Key is updated successfully."

- If your server is activated on the central server, follow these steps:

    1) On the **Security** page, click the **Update Public Key** button to send the update Public Key request to the central server.
    2) When central server admin approves your request, you will see a notification showing "Theft Deterrent server Public Key is updated successfully." on the **Home** page.

Figure 25 - Update Public Key

Then, update the server Public Key on the devices with the following procedures:

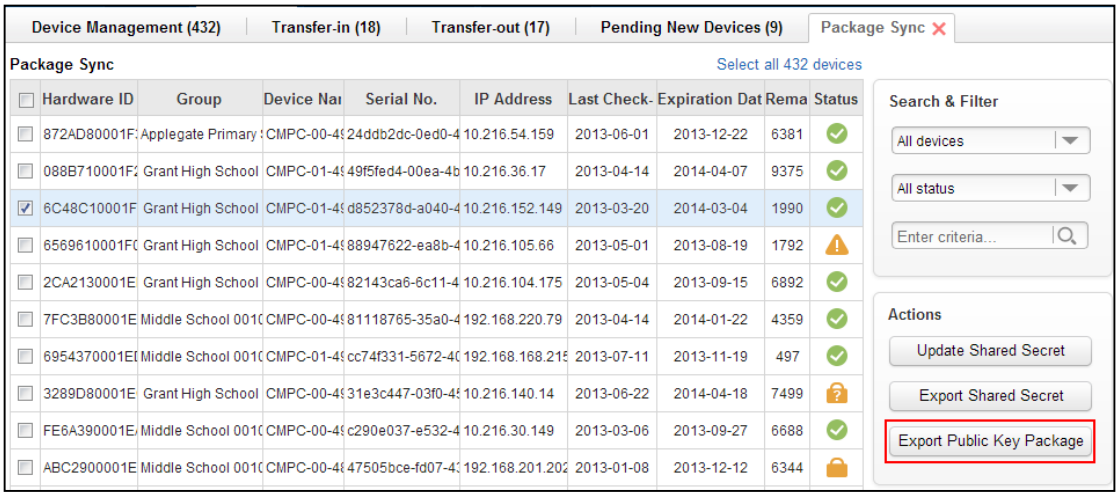
- If the devices are not locked, connect the devices to the server to download and update the server Public Key on the devices automatically.
- If the devices are locked, follow these steps to update the server Public Key on the devices:

    1) On the **Security** page, click the **Synchronize Packages** button.
    2) On the **Package Sync** page, select a device that is locked.

3) Click the **Export Public Key Package** button to export a **tcopp.bin** file to local disk.
4) Copy the **tcopp.bin** file to a removable device.
5) Inset the removable device to the locked device and import the **tcopp.bin** file to update the server Public Key on this device.

Note: You can only select one device to update Public Key offline every time. This update process does not unlock the device.

Figure 26 - Update Public Key Offline



7.4.2 Update Shared Secret

It is recommended that you update the **Shared Secret** of a device when you encounter the following unlock code problems:

- Cannot generate unlock code for the device and the warning message suggests that the **Shared Secret** is invalid or does not exist.
- Failed to unlock the device with the unlock code.

Note: The **Shared Secret** is a 128-digit random number generated by the server for each client. The **Shared Secret** is unique for each client and is stored on both the client and the server.

Steps:

To update the **Shared Secret** of a device, follow this procedure:

Firstly, generate a new **Shared Secret** on the server with the following steps:

1. On the **Security** page, click the **Synchronize Packages** button.
2. On the **Package Sync** page, select the device that you want to update the **Shared Secret** for.
3. Click the **Update Shared Secret** button.

Then, update the **Shared Secret** on the device with this new **Shared Secret** generated on the server. Follow these steps:

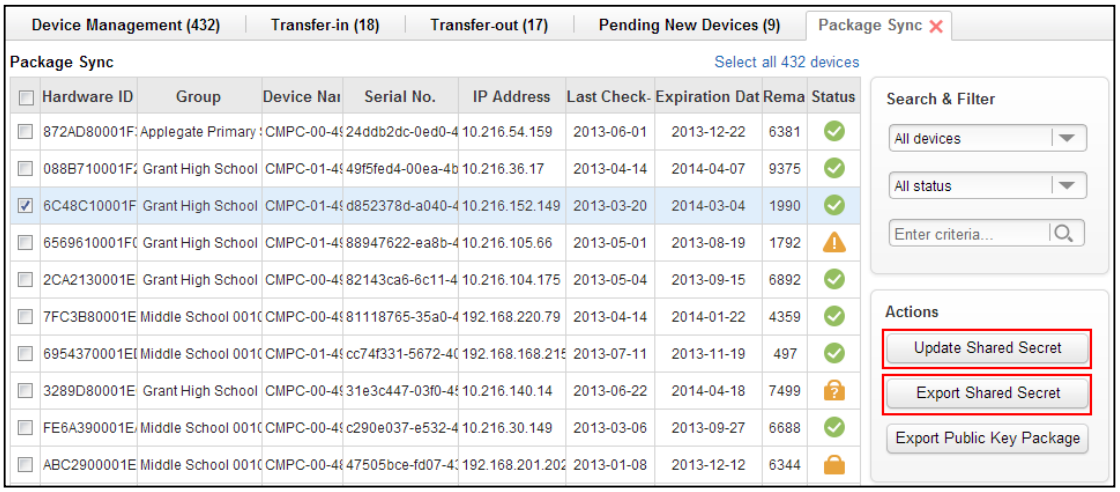
- If the device is not locked, connect the device to the server to download and update the **Shared Secret** automatically.
- If the device is locked, follow these steps to update the **Shared Secret** on the device:

  1) On the **Package Sync** page, select the device that is locked.

2) Click the **Export Shared Secret** button to export a **tcopp.bin** file to local disk.
3) Copy the **tcopp.bin** file to a removable device.
4) Inset the removable device to the locked device and import the **tcopp.bin** file to update the **Shared Secret**.

Note: You can only select one device to export the **Shared Secret** every time. This update process does not unlock the device.

Figure 27 - Update Shared Secret



7.4.3 Export the Public Key

The Server and Root Public Key are required under the following conditions:

- **The server public key:** is required when you generate crash recovery package or pre-activation in the manufactory line.
- **The root public key:** is required when pre-activation in the manufactory line.

Steps:

To export the server and/or root public key, follow these steps:

1. On the **Security** Page, click the **Export** button in the Public Key area.
2. Select the Server Public Key and/or the Root Public Key you want to export.
3. Click the **Export** Button to export the server Public Key (file named as Pub_Key.bin) and/or Root Server Public Key (file named as CmpcRoot.pubkey) to local disk for further use.

Figure 28 - Export the Public Key

7.4.4 Import Pre-activated Package

If some devices are pre-activated in factory with a Public Key not in the server keystore, you must import the pre-activated package to your server to manage these pre-activated devices.

If your server has been activated on the central server, the pre-activated package has been imported to your server during the activation process and no further action is required. Otherwise, you must import the package to the server manually as follows.

For the operation steps of importing Pre-activated Package, please follow the steps of importing Offline Transfer-in Package.

Note: You must not rename the pre-activated package. The package is named as follows: **tcopp_xxxxxxxxxxxxxxxxxxxx_xxxxxxxxxxxxxxxxxxxx.bin**.

After you approve the pre-activated devices, they will download and parse the pre-activated package automatically. You can then manage these devices by using the server.

Note: The pre-activated packages become invalid once the server Public Key is updated. In such cases, follow the steps above to request and import the latest pre-activated package again.

7.4.5 Recover Crashed Server

If your server crashed and the server key pair is lost permanently, install a new server to replace the crashed one by using the crash recovery function.

It is recommended that you use this function only if the server that crashed was running with the **Stand-alone** mode. Otherwise, you can reactivate the new server to replace the crashed one.

Requirements:

To use the crash recovery function, you must obtain the **Provision Number** of the crashed server. The **Provision Number** is a series of characters converted from the server Public Key. You can find the **Provision Number** with the tool provided for the server or on device lock screens.

If the server Public Key has been updated before the server crashed and some devices have not updated their Public Keys accordingly, the server would obtain more than one **Provision Number**.

For the operation steps of importing Crash Recovery Package, please follow the steps of importing Offline Transfer-in Package.

7.4.6 Offline Transfer

If you have Crash recovery or Pre-activate package, which can be used to transfer the device from current TDserver to other TDserver, or from other TDserver to current TDserver, you can enable the Offline Transfer function. If your server is Central Server Supported Mode, the online transfer is enabled at the same time.

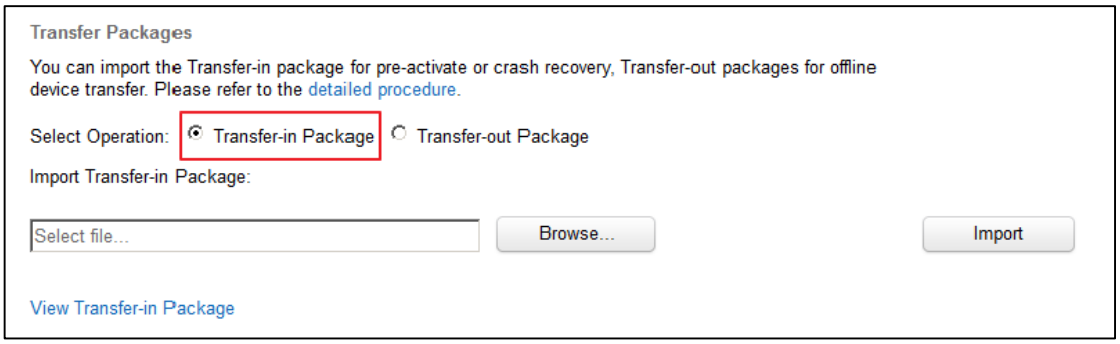
7.4.6.1 Offline Transfer-in

If you want to transfer in some devices from the other or previous crashed server, you can use the offline Transfer-in function with the following steps:

Steps:

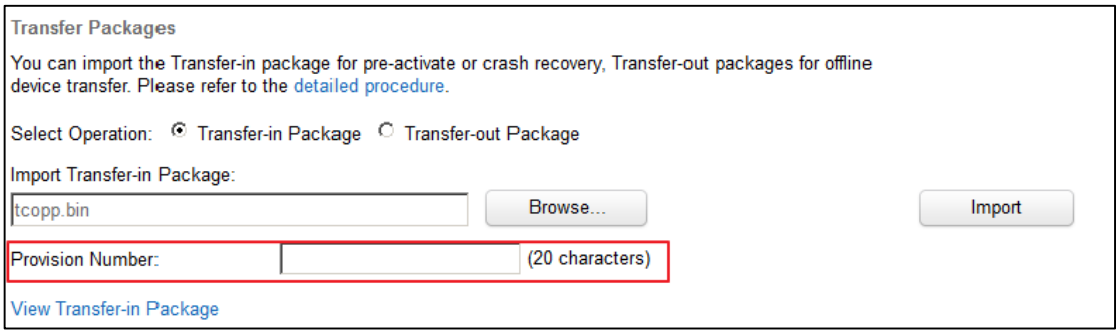
1. On the **Security** page under **Settings**, select **Transfer-in Package** in the **Transfer Packages** area.

Figure 29 – Import Transfer-in Package



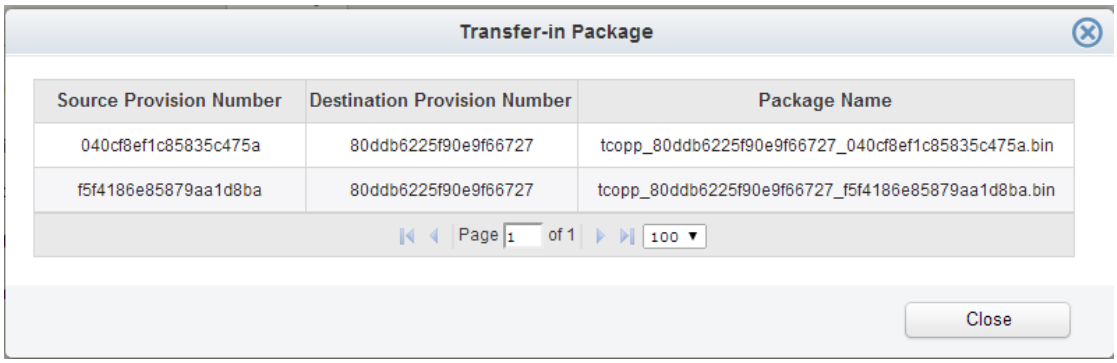
2. Click the **Browse** button to locate the **tcopp.bin** or **tcopp_xxxxxxxxxxxxxxxxxxxx_xxxxxxxxxxxxxxxxxxxx.bin** file. For **tcopp.bin** file, input **Provision Number** in the blank area.

Figure 30 – Import Transfer-in Package



3. Click the **Import** button.
4. You can view all imported transfer-in packages by clicking the **View Transfer-in Package**

Figure 31 – View Transfer-in Package



Note: If a device with unmatched provision number tries to connect with the server, TD server will check whether the transfer-in package applied to the device or not. After the

device successfully downloads and applies the transfer-in package, the device will appear as a new device under **Inventory**.

7.4.6.2 Offline Transfer-out

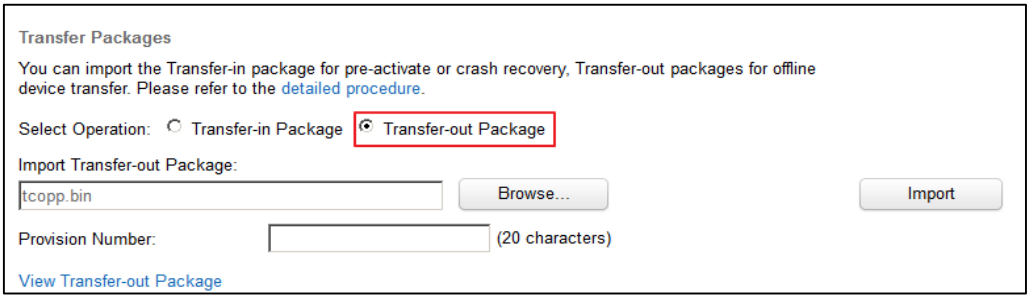
If you want to transfer some devices managed by your TD server to the other server(s), you can use the offline Transfer-out function with the following steps:

Steps:

At first, Import the transfer-out package to your TD server with the following steps:

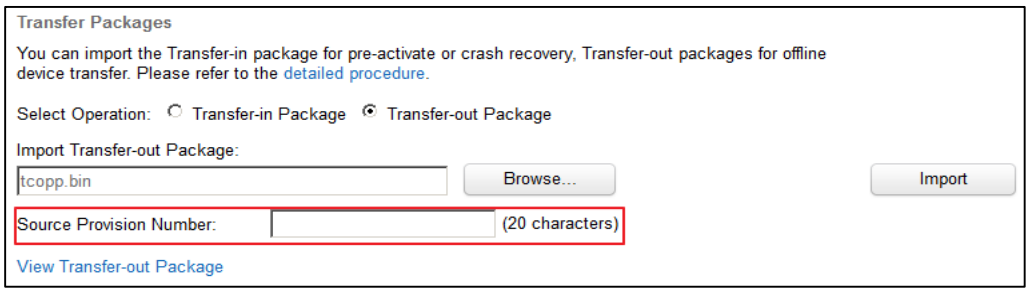
1. On the **Security** page under **Settings**, select **Transfer-out Package** in the **Transfer Packages** area.

Figure 32 – Import Transfer-out Package



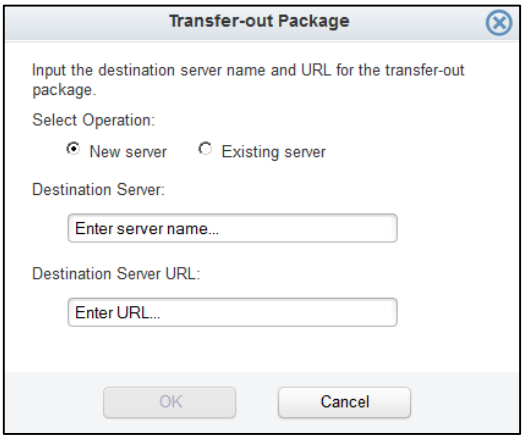
2. Click the **Browse** button to locate the **tcopp.bin** or **tcopp_xxxxxxxxxxxxxxxxxxxx_xxxxxxxxxxxxxxxxxxxx.bin** file. For **tcopp.bin** file, input Provision Number of the **tcopp.bin** in the blank area.

Figure 33 – Import Transfer-out package



3. Click the **Import** button.
4. If there is no existing server relative with the package, you need input the destination server name and URL on the pop-up window.

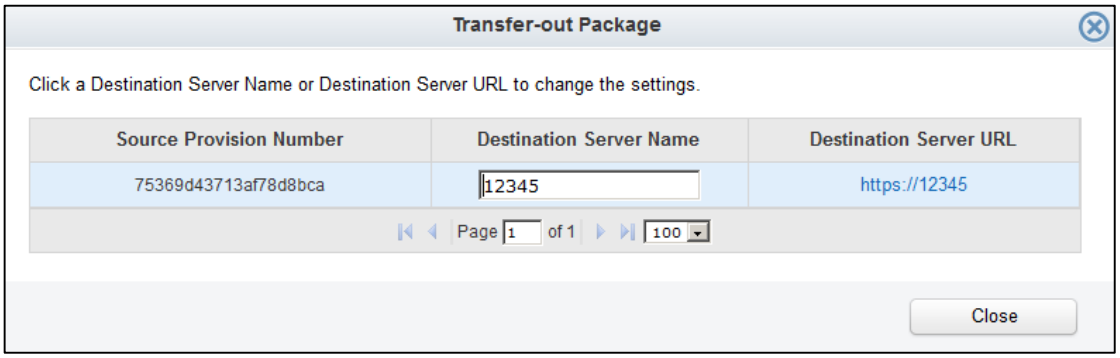
Figure 34 – Input Destination server name and URL



Note: You can overwrite transfer-out package for an existing destination server by selecting the **Existing Server** button in case of Public Key of the server was updated.

5. You can view all imported transfer-out packages by clicking the **View Transfer-out Package.**

Figure 35 – View Transfer-out Package



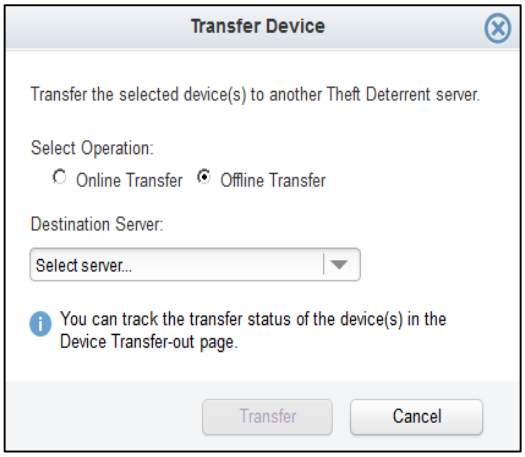
Note: You can click the **Destination Server Name** and **Destination Server URL** to change settings according to the destination server you choose.

Secondly, select the devices you want to transfer out and complete the transfer process with the following steps:

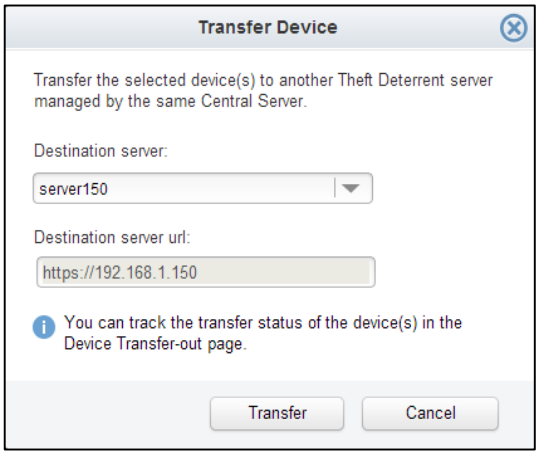
1. On the **Device Management** page under **Inventory**, select the devices you want to transfer out and click the **Transfer** button.
2. On the pop-up window, select **Offline Transfer** if your server is **Central Server Supported mode**. Then select the destination server name and URL, and click **Transfer** button.

Figure 36 – Transfer Device under two modes

With Central Server Supported



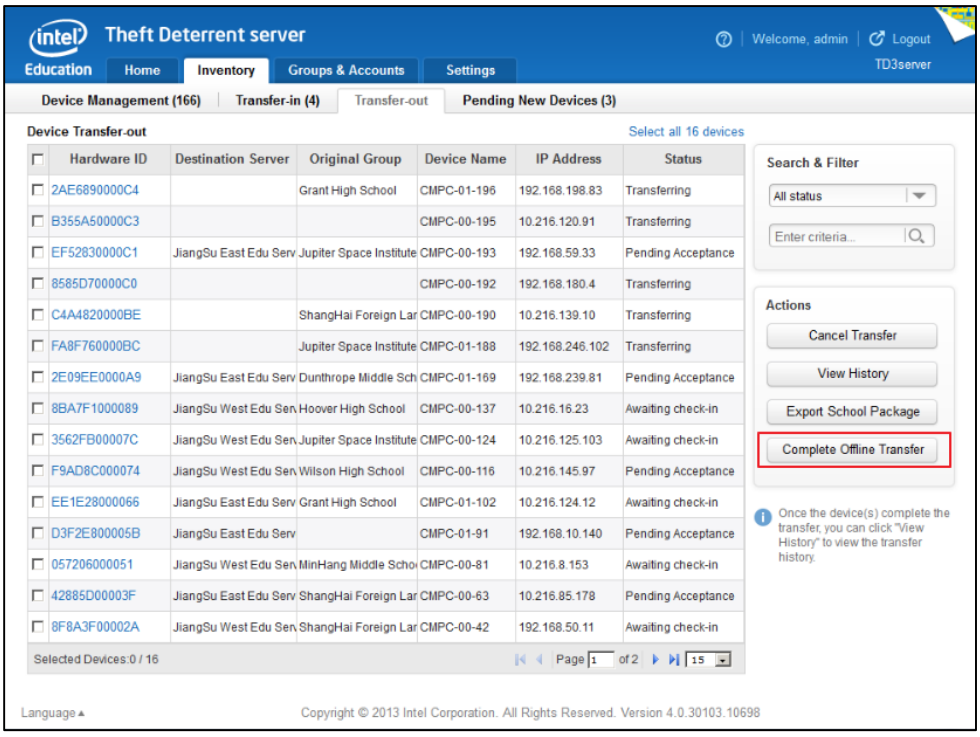
Without Central Server Supported



3. The selected devices will be moved to **Transfer-out** page under **Inventory** with status **Transferring**.
4. Once devices connect with your TD server, they will automatically download the transfer-out packages and their statuses will change to **Downloading**.
5. If the devices reboot and connect with your TD server again, the transfer-out process will be confirmed as complete and these devices will be moved out of device list.
6. Once the device(s) complete the transfer, you can click **View History** to view the transfer history.

Note: You can manually finish transfer by clicking the **Complete Offline Transfer** button in case of any exception happened to block the process complete automatically. Devices with status **Transferring** or **Downloading** will be moved out of device list.

Figure 37 – Transfer-out page



Note: For the devices that are locked and thus cannot connect with the server download the transfer package, you can **Export School Package** and unlock the devices with transfer package.

The device is unlocked after system reboots. You can now manage the device with the new server.

7.5 Advanced Settings

You can only access the **Advanced** page if you logged in as the master admin. On the **Advanced** page, you can configure the following settings:

- Set up server name and address
- Activate the server if installed with the Stand-alone mode with your own Root Public Key
- Reregister the server to register and activate again or Re-activate the server to recover the crashed server

Once the settings are configured correctly, minimal manual changes are needed.

Also, you can access the following functions:

- Back up the server
- Restore the server
- Set up Smart Client Upgrade

7.5.1 Set Up Server Name and Address

The server name and address are usually set up during server pre-configuration. However, if the settings are not yet configured, it is recommended that you set up the server name and address on the **Advanced** page under **Settings**.

Server name

- If the server is activated on the central server, the server name is not editable.

Server address

- Server address is the IP address or URL of the machine that installed the server.
- This server address will be broadcasted to the clients when the Automatic Server Broadcast function is turned on.

Download Log

- Select the log file(s) to compress and then download the compressed log file(s) for trouble shooting.
- Compressing the log file(s) may cause the log files' index disorder, while it will be restored automatically after sometimes.

7.5.2 Activate Theft Deterrent Server (Stand-alone mode & your own Root Public Key)

If your server is installed with the **Stand-alone** mode with your own Root Public Key, you can activate the server with the central server on the **Advanced** page under **Settings**. For more information, see Server Support Mode.

Requirements:

- The server must be connected with the central server through the network.
- The server has never been registered or activated on the central server.

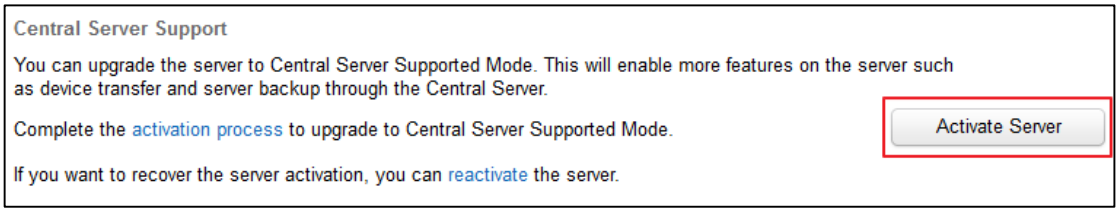
If you had already activated a server that later crashed and would like to replace the crashed server with this newly installed server, see the reactivation steps.

Steps:

To activate the server, follow these steps:

1. On the **Advanced** page under **Settings**, click the **Activate Server** button.
2. Click **Yes** on the confirmation window.
3. On the **Activate Theft Deterrent Server** page (**Step 1**), input all server information and the address of the central server.
4. Click **Register Server** and your activation request is sent to the central server.
5. When your request is approved by the central server admin, you will receive an activation code. The approval process might take a while and you can log out the server during this period.
6. After you receive the activation code, log in the server and click **Register Server** on the **Activate Theft Deterrent server** page (**Step 1**). You can skip this step if you did not log out the server.
7. On the **Activate Theft Deterrent Server** page (**Step 2**), input the activation code and the address of the central server. Then click **Activate Server**.
8. When you see the activation success message, click **OK**.

Figure 38 – Activate Server



The server is transformed to the **Central Server supported** mode after activation completes.

7.5.3 Reregister or Reactivate Theft Deterrent Server

For a server, with either of the following modes, it can be reregistered or reactivated.

- **Stand-alone** mode with your own Root Public Key
- **Central Server supported** mode

Requirements: The server must be connected with the central server through the network.

Re-registration

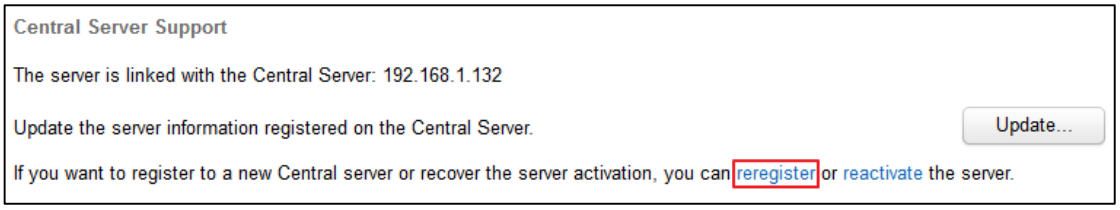
If the current central server deletes your school information, or you want to register to a new central server, you can reregister your server.

Steps:

To reregister the server, follow these steps:

1. On the **Advanced** page under **Settings**, click the **reregister** link in the Central Server Support area.
2. For the following steps, please refer to the 2-8 steps of activating TD server.

Figure 39 – Reregister Server



Re-activation

If an activated server crashed and the server key pair is lost permanently, you can restore the crashed one by reactivating the server.

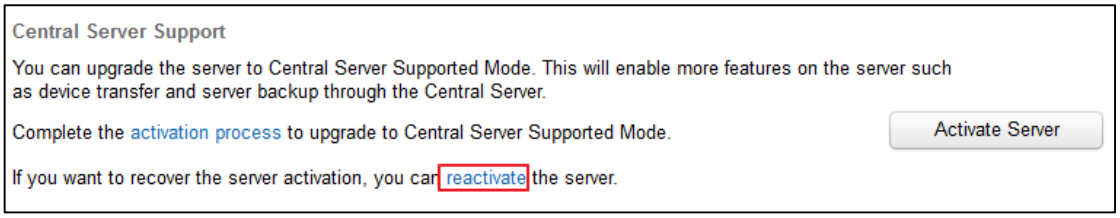
Steps:

To reactivate the server, follow these steps:

1. Contact central server admin offline to request an activation code for reactivation.
2. On the **Advanced** page under **Settings**, click the **reactivate** link.
3. Click **Yes** on the confirmation window.
4. On the **Activate Theft Deterrent Server** page, input the activation code and the address of the central server. Then click **Reactivate Server**.
5. When you see the activation success message, click **OK**.

Note: When reactivation completes, you can approve the devices that were managed by the crashed server when they connect with this server.

Figure 40 – Reactivate Server



Note: After activate or reactivate successfully, usually need restart the Theft Deterrent service before redo activation or reactivation.

7.5.4 Back Up Theft Deterrent Server

On the **Advanced** page under **Settings**, you can back up server data automatically or manually. According to your server support mode, you have the following backup options:

Backup type	*Backup location*	*Server Support Mode*
Automatic	The server machine	All modes
	The central server	Central Server Supported mode only
Manual	The server machine	All modes
	The central server	Central Server Supported mode only

It is recommended that you configure the server to back up data automatically in case the server crashed and you will be able to recover server data with the backup file. The automatic backup occurs at 2:00 AM regularly.

If your server is running the central server supported mode, you can back up server data to the central server. This option is recommended if the central server is accessible to your server and you will be able to retrieve the backup file even if the server machine crashed and lost all data.

Requirements: You must close all the files, folders, and database access tools related to the server.

Steps for Stand-alone Mode:

If your server runs the **Stand-alone** mode, follow these steps to back up your server.

To back up the server automatically, follow these steps:

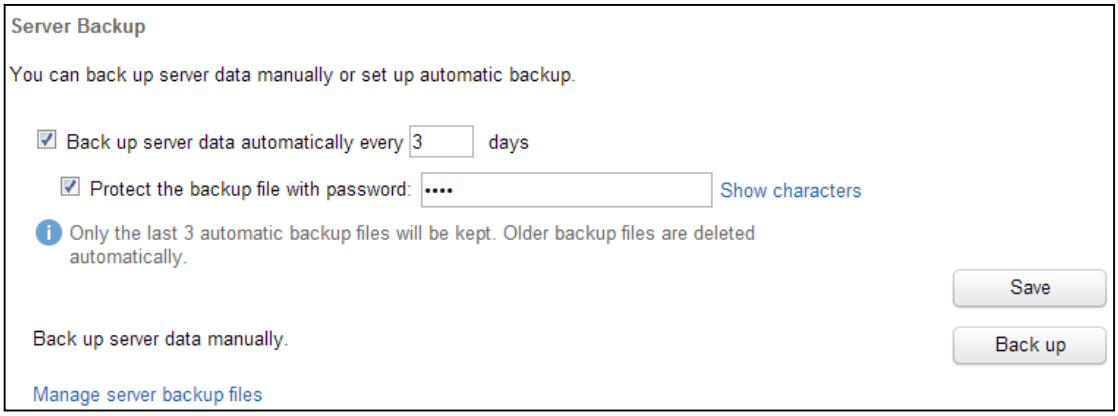
1. On the **Advanced** page under **Settings**, select the **Back up server data automatically** option and input a number to define the frequency of the backup.
2. To protect the backup files with password, select the option and input a password.
3. Click the **Save** button.

Note: The password must be 6 to 30 characters in length. This password will be required when you restore the server.

To back up the server manually, follow these steps:

1. On the **Advanced** page under **Settings**, click the **Back up** button.
2. To protect the backup file with password, select the option and input a password.
3. To save a copy of the backup file to local disk, select the option.
4. Click **Back up**.
5. If you chose to save a copy of the backup file, select a location and save the file.

Figure 41 - Back Up Server with the Stand-alone Mode



Steps for Central Server Supported Mode:

If your server runs the **Central Server Supported** mode, follow these steps to back up your server.

To back up the server automatically, follow these steps:

1. On the **Advanced** page under **Settings**, select the backup options. You can back up the server frequently and back up to the central server.
2. To protect the backup files with password, select the option and input a password.
3. Click the **Save** button.

Note: If you choose to back up the server to the central server, the frequency of the backup is configured by the central server admin. For more information, see the Intel® Education Theft Deterrent Central Server User Manual.

To back up the server manually, follow these steps:

1. On the **Advanced** page under **Settings**, select a manual backup option:

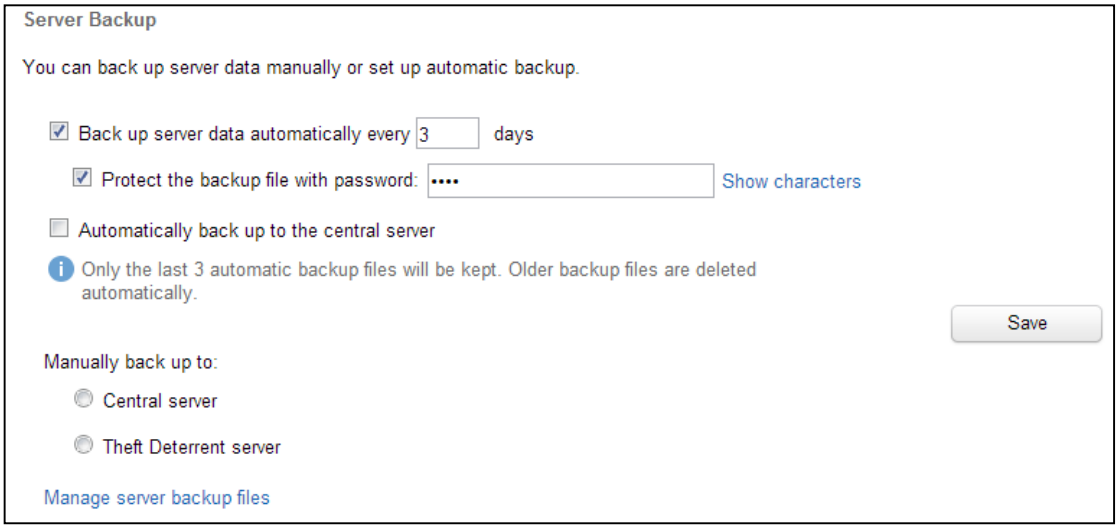
   a) **Central server**: saves the backup file to the central server
   b) **Theft Deterrent server**: saves the backup file to the server machine

2. On the popup window, configure the backup settings:

a) For backup to **Central server**, you can select to save a copy of the backup file to local disk.
b) For backup to **Theft Deterrent server**, you can set a protection password for the backup file and select to save a copy of the backup file to local disk.

3. Click **Back up**.
4. If you chose to save a copy of the backup file, select a location and save the file.

Figure 42 - Back Up Server with the Central Server Supported Mode



7.5.5 Restore Theft Deterrent Server

You can restore the server from an existing backup to recover any lost files or data.

Requirements: You must close all the files, folders, and database access tool related to the server.

Steps:

To restore the server, follow these steps:

1. On the **Advanced** page under **Settings**, click the **Restore** button.
2. Select a restore option:

- **Restore from an automatic backup**: restore from an automatic backup to the server machine
- **Restore from a backup file on server**: restore from a manual backup to the server machine
- **Restore from a restore point on the Central Server**: restore from an automatic or manual backup to the central server
- **Restore from a local backup file**: restore from a copy of a backup file downloaded to local disk

3. Click **Restore**.
4. If you see a popup window requesting the password of the backup file, input the password set during server backup and then click **OK**.
5. Click **Yes** on the confirmation window.
6. After you see the success message, restart the server.

Figure 43 - Restore Server

Note: For server installed with **Central Server supported** mode, if you have updated server Public Key before you restore the server, update server Public Key again once the restore is completed.

7.5.6 Set Up Smart Client Upgrade

You can upload the client upgrade packages to the server to upgrade the clients automatically with the **Smart Client Upgrade** function. For clients of earlier versions, the devices will download and install the upgrade packages when they connect with the server.

According to your server deployment configuration, this function can use the local download feature provided by the server or use a third-party download server.

Requirements: You must have the client upgrade package.

Steps:

To upgrade the clients on devices, follow these steps:

1. Turn on the **Smart Client Upgrade** function on the **Advanced** page under **Settings.**
2. Click the **Upload Package** button to upload the client upgrade package to the server.
3. Select the uploaded package in the table to enable devices to download the package.

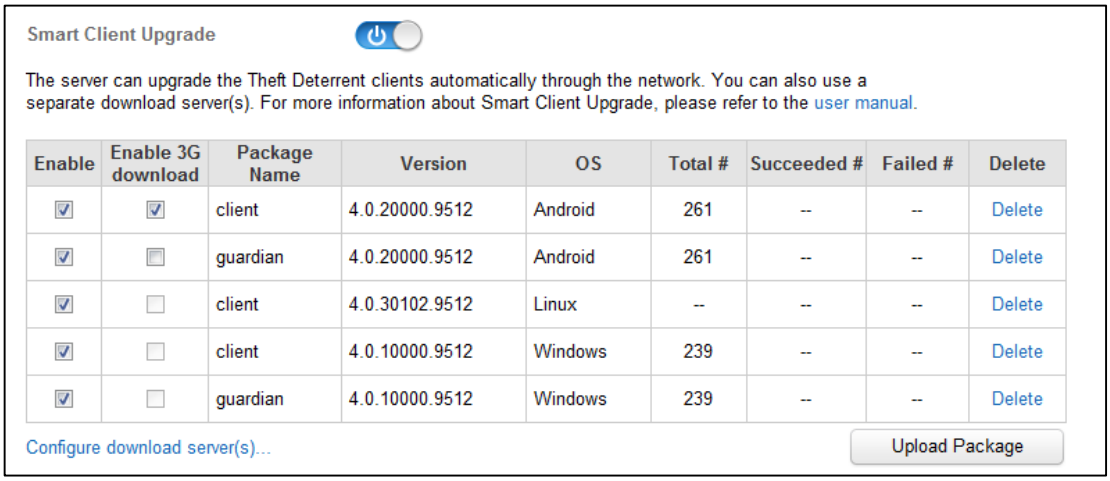
By default, 3G download is not permitted due to the expensive 3G network data consumption. However, you can enable that for mandatory upgrade in Android OS devices.

Note: The upgrade packages should be named according to the following naming rules.

Version	*OS*	*Display Name*	*File name*
4.0.10000.XXXX	Windows	client	Theft_Deterrent_client_v4.0.10000.XXXX.release.zip
4.0.10000.XXXX	Windows	guardian	Theft_Deterrent_guardian_v4.0.10000.XXXX.release.zip
4.0.3010X.XXXX	Linux	client	Theft_Deterrent_client_v4.0.3010X.XXXX.release.zip
4.0.3010X.XXXX	Linux	guardian	Theft_Deterrent_guardian_v4.0.3010X.XXXX.release.zip
4.0.20000.XXXX	Android	client	Theft_Deterrent_client_v4.0.20000.XXXX.release.zip

The devices will download and install the upgrade packages when their current client versions are earlier than the versions of the packages.

Figure 44 - Smart Client Upgrade



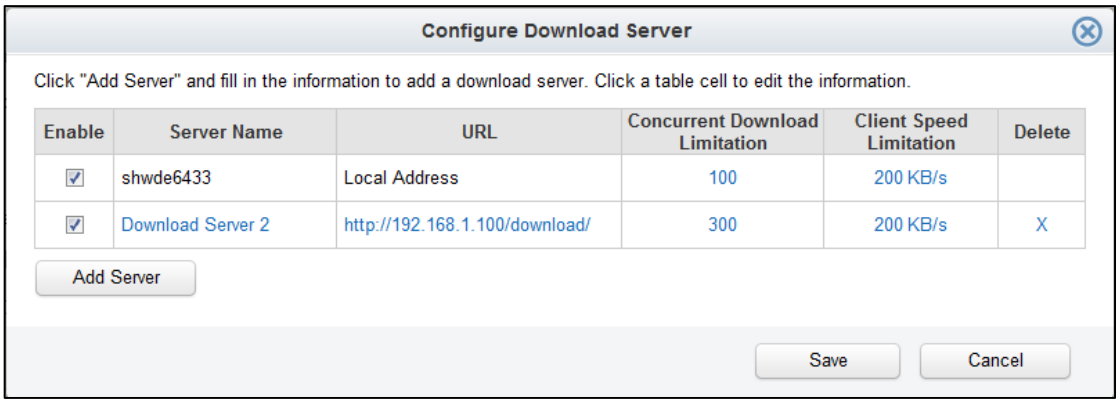
For devices to download the upgrade packages smoothly, server is configured with either the local download feature or a separate download server during deployment. However, if this setting is not configured correctly during deployment or if you want to add a download server, click the **Configure download server(s)** link and then input the following information:

- **Server Name**: the name of the download server.
- **URL**: the URL of the download server, which must be in HTTP scheme. For example, http://192.168.1.100/download/
- **Concurrent Download Limitation**: the maximum number of devices that can download the upgrade packages at the same time.
- **Client Speed Limitation**: the maximum network speed for a device to download the upgrade packages.

You can select one or multiple download servers to implement the download function at the same time. The local server is the local download feature provided by default.

Note: When you add, edit, or delete a download server, the configuration takes effect only after you click the **Save** button.

Figure 45 - Configure Download Server



For the separate download server, the client update package must be manually copied under download URL, with the same file name as the local download server under:

- **Debian**: `/opt/TheftDeterrentServer/Site/welcome-content/tdupdate`
- **Windows**: `C:\Program Files\Intel Education Software\Theft Deterrent server\Site\webapps\tdupdate`

7.6 Account Settings

If you logged in the server with a helpdesk/call center or customer account, you can edit your account information on the **Account** page under **Settings**.

Note: If you logged in as the master admin or a program admin, you can edit your account information on the **Accounts** page under **Groups & Accounts**.

Steps:

To edit your account information, open the **Account** page either by clicking **Settings** -> **Account** or by clicking your username on the upper-right corner of the webpage.

Figure 46 - Account page

8. Troubleshooting

8.1 Warning and Error Messages

If you see a device record displayed in orange (Warning) or red (Error) on the server webpage, check the following solutions.

Page	*Issue*	*Warning/Error*	*Solution*
Device Management	Boot Tick inconsistent	Warning	Reset the Boot Tick on the **Device Details** page.
	Download limit expired	Warning	Reset the download limit on the **Device Details** page
	Device hardware error	Error	Check the error codes.
Transfer-in	Transfer error	Error	Reject the device.
Pending New Devices	Client with earlier version	Warning	Check the client status. If the client is in **Inactive** status or is pre-activated with a Public Key related to this server, approve the device. Otherwise, reject the device.
	Device hardware error	Error	Reject the device.

8.2 Device Error Codes

The following error codes are displayed on the **Device Details** page or in the notifications when the device has hardware error.

Device Error Code	*Description*
0X02010001	The TPM device cannot be found.
0X02010002	The TPM is disabled.
0x02011006	
0X02010003	The TPM is deactivated.
0x02011007	
0X02010004	Error occurred during TPM initialization in the manufactory line. The possible reasons include the following: 1. The TPM does not have an Endorsement Key pre-installed. 2. The TPM NV partition or NV index creation failed. 3. The TPM status is incorrect.
0X02010005	
0X0201000A	
0X0201000C	
0X0201000E	
0X0201000F	
0X02011003	Error occurred try to provision TD in the device. The possible reason

	is the failed to set the TPM flag.
0X0201EEEE	The TPM status error is reported by an old version of TD client (2.x)
0X0201FFFF	Internal error accessing the TPM.

8.3 Client Unlock Screen Error Codes

The following error codes are displayed on the client unlock screen, describing the detailed reasons of unlocking failure during **Unlock through Network**:

Unlock Screen Error Code	*Description*
0x01040002	Cannot connect with the server. Please check the server address or AP access.
0x01040040	The server address is invalid because it is shorter than 4 characters.
0x01040080	Cannot connect with the server because the proxy username or password is invalid.
0x01060002	The server address is empty.
0x04020001	Server is error.
0x04020003	Server is busy. Please try again later.
0x04020004	Server is under maintenance. Please try again later.
0x04070001	Cannot unlock this device because it is not managed by the server yet.
0x04070002	Cannot unlock this device because it is still waiting for the server's approval.
0x04070003	Cannot unlock this device because it has been rejected by the server.
0x04070005	Connected to the wrong server. (The Root Public Key in the server is not the same as that in the device)
0x04070006	Connected to the wrong server. (The server Public Key is not the same as that in the device)
0x04070007	Failed to unlock the device because the Boot Tick in the client is inconsistent with that in the server.
0x04070008	Failed to unlock the device because the certificate download limit exceeded the threshold in the server.

8.4 Smart Client Upgrade Error Codes

If **Smart Client Upgrade** failed, click the **Failed** link and then check the error codes in the following table.

Error Codes	*Descriptions*
0x02050002	Failed to download the upgrade package. The error might be caused by network problems.
0x02050008	The update package is corrupt.

0x02050010	Each upgrade package can only contain one file (.exe or .apk).
0x02050040	Fail to run the upgrade package. For example, the .exe file or the .apk file in the package is broken.

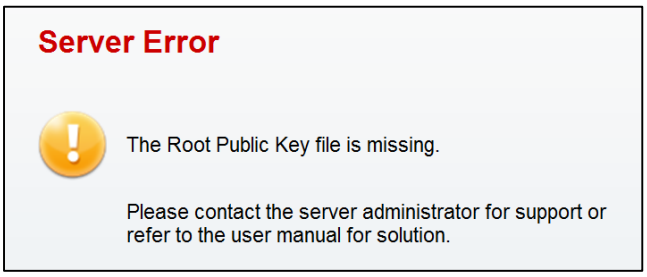
8.5 Register/Activate Error Codes

If **register/activate** failed, the error code will display in the popup error dialog.

Error Codes	*Descriptions*
0x05028001	Central server is under maintenance mode.
0x05068003	The activation code is invalid.
0x05068004	Retry to reactivate with the activation code used to activate in previous.
0x05068005	The central server cannot connect with Root CA server.
0x05068006	Cannot register again for the server already being registered and activated.

8.6 The Root Public Key file is missing

Figure 47 - Server Error (1)



As master admin, if you see this error message on the **Login** page, follow one of these solutions according to your server support mode.

- If your server is installed with the **Stand-alone** mode with your own Root Public Key, rename your Root Public Key to **td-cert-root.pubkey** and then copy it to the following directory on the machine that installed the server.

  Windows: `C:\Program Files\Intel Education Software\Theft Deterrent server\Site\domain\data\security`
  Debian: `/opt/TheftDeterrentserver/Site/domain/data/security`

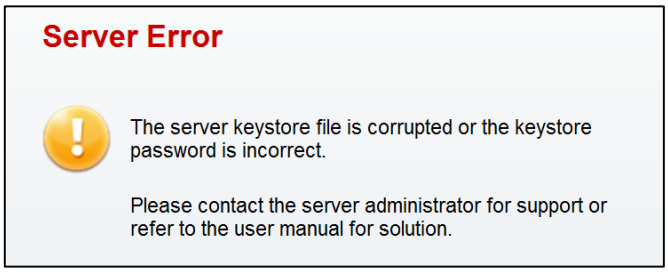
- If your server is installed with the **Central Server supported** mode, re-install the server and then reactivate the server during pre-configuration.
- If your server is installed with the **Stand-alone** mode with the Intel Root Public Key, follow these steps:

  1) Install the server with the **Stand-alone** mode on another machine.
  2) Copy the **td-cert-root.pubkey** file from the new server to your original server in the following directory:

     Windows: `C:\Program Files\Intel Education Software\Theft Deterrent server\Site\domain\data\security`
     Debian: `/opt/TheftDeterrentserver/Site/domain/data/security`

8.7 The server keystore file is corrupted

Figure 48 - Server Error (2)



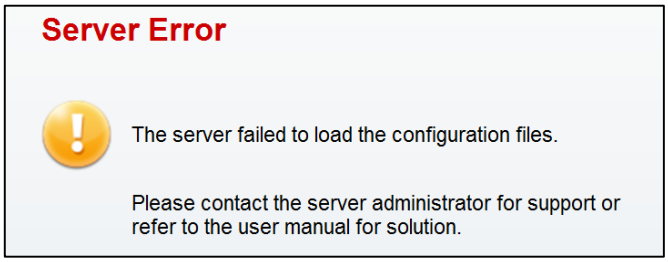
As master admin, if you see this error message on the **Login** page, re-install the server and then restore it with a backup file.

However, if you have not backed up your server, follow one of these solutions according to your server support mode.

- If your server is running with the **Central Server supported** mode, re-install the server and then reactivate the server
- If your server is running with the **Stand-alone** mode, re-install the server and then import a crash recovery package.

8.8 The server failed to load configuration files

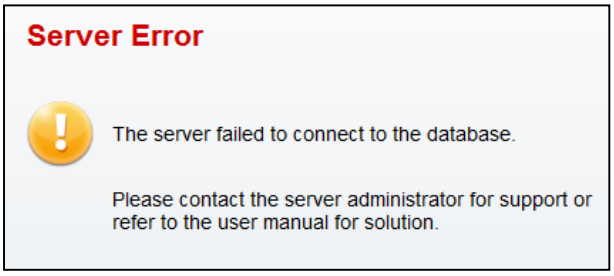
Figure 49 - Server Error (3)



As master admin, if you see this error message on the **Login** page, follow the solutions in The server keystore file is corrupted.

8.9 The server failed to connect to the database

Figure 50 - Server Error (4)



As master admin, if you see this error message on the **Login** page, restart the server with the following steps:

- **Windows**: Click **Start** menu -> **All Programs** -> **Intel Education Software** -> **Theft Deterrent server** -> **Start Server**.

- **Debian**: Restart the server by running this command with root privilege:

```
service theftdeterrentserver restart
```

Also, if your server is installed with a separate database, make sure that the network connection between the web server and the database server is correct.

8.10 Error 404: Page not found

As master admin, if you see the 404 error message, refresh the webpage or return to the login page to log in the server again. Also, make sure that you input the correct URL.

If the problem remains, restart the server with the following steps:

- **Windows**: Click **Start** menu -> **All Programs** -> **Intel Education Software** -> **Theft Deterrent server** -> **Start Server**.
- **Debian**: Restart the server by running this command with root privilege:

```
service theftdeterrentserver restart
```

Also, make sure that the server is connected to the network correctly.

8.11 Theft Deterrent server activation problem

If you failed to activate TD Server, ensure that the network connection between TD Server and the central server is successfully and then check the following items.

If your activation failed on step 1 (the registration step), do the following:

- Make sure that you input the correct address of the central server.
- Contact the central server admin to ensure that your server machine has never been activated on the central server. Otherwise, reactivate the server.

If your activation failed on step 2 (the activation step), do the following:

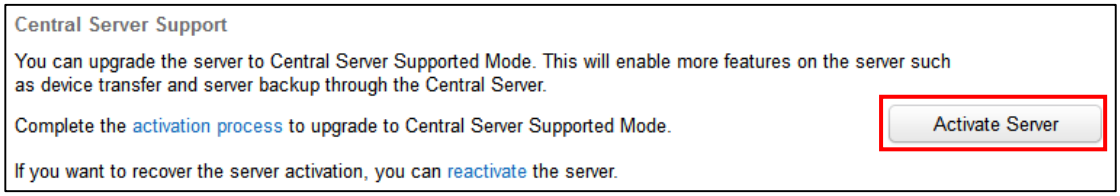
- Make sure that you input the correct activation code.
- If your server is installed with the **Stand-alone** mode, make sure that your server is imported with the correct Root Public Key during installation.

9. FAQ

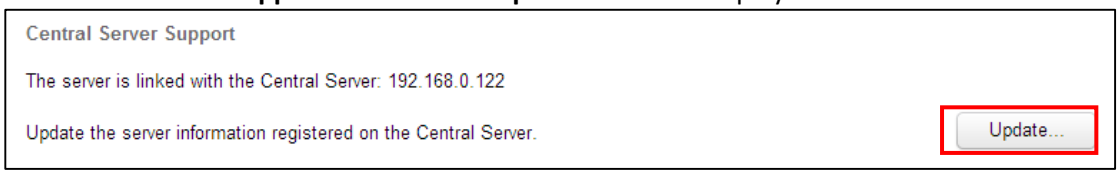
1. How do I find out the server support mode of my server?

Answer: During the deployment of the server, either of following server support mode is selected: **Stand-alone** or **Central Server supported** mode. To find out the server support mode, open the **Advanced** page under **Settings** and check the **Central Server Support** area.

- **Stand-alone** mode with Intel Root Public Key: the webpage does not contain such an area.
- **Stand-alone** mode with your own Root Public Key: the **Activate Server** button is displayed as follows:



- **Central Server supported** mode: the **Update** button is displayed as follows:



2. How do I find the version of the server?

Answer: The server version number is displayed at the bottom of the server webpage.

3. How do I start, stop, and restart the server as well as check server status?

Answer: The steps differ according to the server operating system:

- **Windows**: Click **Start** menu -> **All Programs** -> **Intel Education Software**-> **Theft Deterrent server** -> click **Start Server**, **Stop Server** or **Check Server Status**.
- **Debian**: Run following commands with root privilege:

```
service theftdeterrentserver start
service theftdeterrentserver stop
service theftdeterrentserver restart
service theftdeterrentserver status
```

Note: In Windows, if the server is running, you can restart the server by clicking the **Start Server** option. If the server is installed with a separate database, make sure that you run the command on both the web server and the database server.

4. What do I do if the server webpages are distorted?

Answer: First of all, make sure that your web browser is supported by the server by checking the browser requirements. Also, it is recommended that you clear the cache, cookies and history in your browser regularly.

If you are browsing with IE in Windows Server 2008, click **Tools** -> **Internet Options** -> **Security** tab and change the security level to medium-low.

5. Why are some device records shown in orange/red?

Answer: A device record in orange or red indicates a warning or error message for the device. For more information, see Warning and Error Messages.

6. What do I do if server restore failed?

Answer: Close all the files and database access tools related to the server as well as the following folders and then restore the server again:

Windows: `C:\Program Files\Intel Education Software\Theft Deterrent server`

`C:\ProgramData\TheftDeterrent2`

Debian: `/opt/TheftDeterrentserver`

`/etc/TheftDeterrent2`

7. What do I do if the language displayed on the webpage is incorrect?

Answer: If the language displayed on the webpage is not the one selected, re-selected the language from the **Language** list on the button left-side of the webpage.

8. What do I do if I see a message saying the server is under maintenance?

Answer: Wait for the master admin to complete the server pre-configurations and then log in the server again.

9. Why do I see many e-mail error notifications?

Answer: This might be because the e-mail server is not configured correctly. Check the e-mail settings on the **Server** page under **Settings** by clicking the **Test** button. If connection failed, correct the e-mail server settings or turn off the e-mail server function.

10. What do I do if I see a notification saying server backup failed?

Answer: This notification indicates that the last automatic backup failed. Make sure that your machine has enough hard disk space for backup and close any database management tools connected to the server database. This notification is displayed until the next automatic backup.

11. Why does the client ignore some certificates?

Answer: A client might be provisioned with different certificates but can only download one certificate each time according to certain orders:

Kill pill (manual lock) > Global Certificate > all other certificates

For example, if a client in **About to Expire** status is provisioned with a Permanent Certificate, the client will download the Permanent Certificate only after it downloads and applies the Global Certificate.

10. Glossary

Theft Deterrent client (client): The software that is installed in the devices and is the communication link between the server and the device.

Central server: The server that manages the Theft Deterrent servers and acts as the link between the root CA server and the Theft Deterrent servers.

Root CA server: The server that creates and signs Root Public Key and Digital Certificates.

Server Public Key: The public key file of the Theft Deterrent server, which is unique for each server.

Root Public Key: The public key file of the root CA server.

Expiration Date: The date from which the device will be locked.

Remaining Cycles: The number of times that a device can reboot or restore from sleep or hibernate before it is locked. This is not applicable to Intel® Education Tablet.

Shared Secret: A 128-digit random number generated by the server for each client soon after the client account is created. It is only used for verifying Unlock Codes when unlocking devices.

Provision Number: A 20-digit hexadecimal number generated from the server Public Key.

Unlock Code: A 10-digit number generated by the server for unlocking a device.

Appendix A. Device Status

Status name	*Status icon*	*Description*
Normal		The client is working correctly.
Permanent		The client is working correctly. Its **Expiration Date** and **Remaining Cycles** are set to a value that will never expire.
About to Expire		The device will be locked in a few days or after a few boots, sleep, or hibernation.
Lock Pending		The device will receive a kill pill and be locked once it connects with the server.
Manually Locked		The device is manually locked.
Automatically Locked		The device is locked because the **Expiration Date** has expired.
Unlock Pending		The device has been allowed unlocking.
Awaiting check-in		The device is awaiting for check-in
Error		The client has error.

Appendix B. Notification Table

Type	*Category*	*Description*	*Action*
Error	Server Backup	Last automatic backup (to central server) failed at [date]: Backup now.	Check the status of the server and retry the server backup or restore
	Server Restore	Last restore failed at [date].	
	Server Update	Theft Deterrent server Public Key was updated failed at [date].	Check the connectivity with the central server.
	Server Connection	Failed to connect with the Central Server; last connection: [date].	
	Server Registration	The server registration was rejected by the Central Server at [date].	Connect with the central server admin.
	Device Error	XXX device(s) has error.	Refer to the device error code and find the device to debug. For managed device, the error can be cleared.
Warning	E-mail	Failed to send [email type] to [receiver] by e-mail at [date].	Check the email server availability.
	Device Transfer-in	XXX device(s) is being transferred to this server and requires your approval.	Approve or reject the transfer.
	Device Transfer-out	The transfer request(s) of XXX device(s) has been rejected by the destination server(s) since your last login.	Connect with the destination server admin.
	Pending New Device	XXX new device(s) needs your approval.	Approve or reject the device.
	Awaiting check-in	XXX new device(s) has been approved under awaiting for check-in.	Wait for the device to check-in the server.
	Device Status	XXX device(s) has been locked since your last login.	1. If the device number is reasonable, generate unlock code for these device 2. If the device number is not reasonable, check the server status and network connectivity.
	Device Status	XXX device(s) will expire in 7 days.	
	Device Status	XXX device(s): The Boot Tick at the client side is inconsistent with that in the server.	Reset the boot tick.
	Device Status	XXX device(s): The number of certificates downloaded has exceeded the boot certificate limit.	Reset the certificate download limit.

Information	Server Backup	Last automatic backup (to central server) was successful at [date].	No action is required.
	Server Restore	Last restore was successful at [date].	
	Server Update	Theft Deterrent server Public Key was updated successfully at [date].	
	Server Connection	The connection with the Central Server was successful; last connection: [date]	
	Server Registration	The server registration was accepted by the Central Server at [date]	
	New Device	XXX new device(s) has been added since your last login.	
	Device Transfer-out	XXX device(s) has been transferred to other server(s) successfully since your last login.	
	Device Transfer-out	XXX device(s) is pending to be transferred to other server(s).	